

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-040753

(43)Date of publication of application : 05.02.2004

(51)Int.Cl. H04N 1/387
G06F 17/60
G06T 1/00
G09C 5/00
G10L 11/00
H04L 9/36
H04N 7/08
H04N 7/081
H04N 7/30

(21)Application number : 2002-362515 (71)Applicant : SONY UNITED KINGDOM LTD

(22)Date of filing : 13.12.2002 (72)Inventor : PELLY JASON CHARLES
TAPSON DANIEL WARREN

(30)Priority

Priority	2001	200129841	Priority	13.12.2001	Priority	GB
number :			date :		country :	

(54) DATA PROCESSING APPARATUS AND DATA PROCESSING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a watermark system immune to attacks.

SOLUTION: An encoded data processing apparatus is provided for creating a watermarked copy of an original material item by introducing one code word in a set of prescribed code words to a copy of a material item. Each of code words in the set of code words is intrinsically related to a data word having first and second fields. Each of values in a set of values of the first and second fields is represented as a first part of a code word having a first plurality of coefficients and a second part of a code word having a second plurality of coefficients. By generating the watermark code word having the first and second parts, data words in the first and second fields are individually identified. The first and second fields are related to different parameters such as address parameters, for example.

LEGAL STATUS

[Date of request for examination] 26.10.2005

[Date of sending the examiner's decision
of rejection]

[Kind of final disposal of application other
than the examiner's decision of rejection
or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1]

In the coded data processor which generates the copy to which the water mark of an original material item was given by introducing one codeword in the group of a predetermined codeword into the copy of a material item,

The codeword generation machine which generates the above-mentioned codeword which has two or more codeword multipliers,

It has the coding processor which combines the above-mentioned codeword multiplier with the above-mentioned material item,

It is the coded data processor with which each codeword of the group of the above-mentioned codeword is related with the data word which has the 1st and 2nd fields by the proper, and each value of the group of the value of these 1st and 2nd fields is expressed as the 2nd part of the above-mentioned codeword which has the 1st part of the above-mentioned codeword which has two or more 1st multipliers, and two or more 2nd multipliers.

[Claim 2]

Each value of the 1st field of the above is a coded data processor according to claim 1 characterized by what is expressed as a cyclic predetermined shift of two or more 1st codeword multipliers of the 1st part of the above-mentioned codeword.

[Claim 3]

The value of the 1st field of the above is a coded data processor according to claim 2 characterized by defining the shift with predetermined [of the codeword multiplier of the above 1st / the above-mentioned codeword generation machine is equipped with the pseudo-random number generation machine which generates the pseudo-random number from which the 1st part of the above-mentioned codeword is drawn, and cyclic].

[Claim 4]

They are claim 1 which two or more 2nd multipliers of the 2nd part of the above-mentioned codeword are drawn from the pseudo-random number generated using the auxiliary seed value specified with the value of the 1st field of the above among two or more seed values, and is characterized by expressing each value of this 2nd field as a shift to which the multiplier of this 2nd plurality corresponds thru/or a coded data processor given in 3 any 1 terms.

[Claim 5]

The above-mentioned codeword generation machine is claim 1 characterized by generating the 1st seed value for generating two or more above-mentioned codeword multipliers from the sample of the above-mentioned material item thru/or a coded data processor given in 4 any 1 terms.

[Claim 6]

The above-mentioned coding processor is claim 1 characterized by the thing of two or more codeword multipliers of the above 1st, and two or more codeword multipliers of the above 2nd for which one of sequence is changed at least thru/or a coded data processor given in 5 any 1 terms based on a sequence modification code.

[Claim 7]

The discrete cosine transform processor which changes the above-mentioned material item into a discrete cosine transform field,

The material item of the above-mentioned discrete cosine transform field It is expressed by two or more discrete cosine multipliers. The above-mentioned coding processor By adding one of the above-mentioned codeword multiplier and the

corresponding discrete cosine transform multipliers By combining the above-mentioned codeword multiplier and the above-mentioned material item, and carrying out the reverse discrete cosine transform of the image with which the above-mentioned codeword was added by this coding processor and by which the discrete cosine transform was carried out [above-mentioned] A coded data processor [equipped with the reverse discrete cosine transform processor which generates the version to which the water mark of the above-mentioned material item was given] according to claim 6 or 7.

[Claim 8]

Projection equipment equipped with claim 1 which at least one of an audio signal and picture signals is supplied, and introduces a codeword into at least one of this audio signal and picture signals before copy processing thru/or a coded data processor given in 7 any 1 terms.

[Claim 9]

A web server equipped with claim 1 which it is the web server which offers the material item downloaded through the Internet, this material item is supplied before this material item downloads, and introduces a codeword into this material item thru/or a coded data processor given in 7 any 1 terms.

[Claim 10]

It is the detection data processor which specifies at least one codeword which exists in the version to which the water mark of a material item was given among the groups of a codeword. The version to which this water mark was given to each sample of two or more samples of the original version of this material item It is generated by combining one codeword multiplier to which it corresponds of two or more codeword multipliers. Each codeword multiplier It is related with the data word which has the 1st and 2nd fields by the proper. Each value of the group of the value of this 1st field It is expressed as the 1st part of the above-mentioned codeword which has two or more 1st multipliers. This 2nd field In the detection data processor with which it is expressed as the 2nd part of the above-mentioned codeword which has two or more 2nd multipliers, and each value of the 1st field of the above is expressed as a cyclic predetermined shift of two or more 1st codeword multipliers of the 1st part of the above-mentioned codeword,

The decode processor which reproduces a codeword from the material item to which the above-mentioned water mark was given, and generates a playback codeword,

The 1st part of the above-mentioned playback codeword is made to correlate with the 1st part of each codeword generated from the group of a codeword, and a correlation value is computed about each generated codeword,

The value of the 1st field is detected from the corresponding correlation value exceeding a predetermined threshold,

It is made to correlate with the 2nd part of each codeword generated from the group of the above-mentioned codeword of the 2nd part of the above-mentioned playback

codeword, and the 2nd correlation value is computed about each generated codeword,

A detection data processor equipped with the detection processor which detects the value of 1st at least one data field, and the value of 2nd at least one data field by detecting the value of the 2nd field from the 2nd corresponding correlation value exceeding a predetermined threshold.

[Claim 11]

The above-mentioned detection processor,

The Fourier transform value of the part corresponding to the 1st part of the above-mentioned playback codeword is computed,

The Fourier transform value of two or more 1st codeword multipliers of the 1st part of the codeword by which generation was carried out [above-mentioned] is computed,

The complex conjugate of either the Fourier transform value of the 1st part of the above-mentioned playback codeword or the Fourier transform value of the 1st part of the codeword by which generation was carried out [above-mentioned] is computed,

The 1st middle product sample is computed by carrying out the multiplication of the Fourier transform sample of the 1st part of the above-mentioned playback codeword, and the Fourier transform sample of the 1st corresponding part of the codeword by which generation was carried out [above-mentioned],

The detection data processor according to claim 10 characterized by computing a correlation value with the value of the 1st part of each codeword by which carried out inverse transformation of the above-mentioned middle product sample, and generation was carried out [above-mentioned] with the value of the 1st part of the above-mentioned playback codeword by computing the correlation sample to which each expresses the correlation value of the 1st part of the above-mentioned codeword.

[Claim 12]

Two or more 2nd multipliers of the 2nd part of the above-mentioned codeword are drawn from the pseudo-random number generated using the auxiliary seed value specified with the value of the 1st field of the above among two or more seed values, and each value of this 2nd field is expressed as a shift to which the multiplier of this 2nd plurality corresponds,

The above-mentioned decode processor specifies the auxiliary seed value shown from the group of an auxiliary seed value with the value of the 1st field detected from the above-mentioned correlation value,

The above-mentioned detection processor is a detection data processor according to claim 10 or 11 characterized by generating two or more codeword multipliers of the above 2nd, and specifying the value of the 2nd data field of the above from the shift of the codeword multiplier of the above 2nd to the 2nd part of the above-mentioned playback codeword from the auxiliary seed value by which specification

was carried out [above-mentioned].

[Claim 13]

The above-mentioned detection processor is a detection data processor according to claim 12 characterized by specifying the value of the shift of two or more 2nd generated this multipliers to the 2nd part of this playback codeword by making two or more 2nd multipliers by which generation was carried out [above-mentioned] correlate with the 2nd part of the above-mentioned playback codeword.

[Claim 14]

The above-mentioned detection processor,

The Fourier transform value of the part corresponding to the 2nd part of the above is computed,

The Fourier transform value of two or more 2nd codeword multipliers of the 2nd part of the codeword by which generation was carried out [above-mentioned] is computed,

The complex conjugate of either the Fourier transform value of the 2nd part of the above-mentioned playback codeword or the Fourier transform value of the 2nd part of the codeword by which generation was carried out [above-mentioned] is computed,

The 2nd middle product sample is computed by carrying out the multiplication of the Fourier transform sample of the 2nd part of the above-mentioned playback codeword, and the Fourier transform sample of the 2nd corresponding part of the codeword by which generation was carried out [above-mentioned].

The detection data processor according to claim 13 characterized by making two or more 2nd multipliers by which carried out inverse transformation of the above-mentioned middle product sample, and generation was carried out [above-mentioned] by computing the correlation sample to which each expresses the correlation value of the 2nd part of the above-mentioned codeword correlate with the 2nd part of the above-mentioned playback codeword.

[Claim 15]

It is the detection data processor of claim 10 to which either at least is embedded to a material based on a sequence modification code, and the above-mentioned compound processor is characterized by the thing of the playback codeword multiplier of the above 1st and the above 2nd for which one of sequence is returned at least based on this sequence modification code thru/or 14 any 1 term publication of two or more codeword multipliers of the above 1st, and two or more codeword multipliers of the above 2nd.

[Claim 16]

They are claim 10 to which either at least is embedded to a material based on a sequence modification code, and the above-mentioned detection processor is characterized by the thing of the codeword multiplier by which the above 1st and the 2nd were generated based on this sequence modification code of two or more codeword multipliers of the above 1st, and two or more codeword multipliers of the

above 2nd for which one of sequence is returned at least thru/or a detection data processor given in 14 any 1 terms.

[Claim 17]

In the addressee specification system which specifies the addressee of a material item,

Claim 1 which generates the material item to which the water mark was given by introducing into a material item the codeword generated from the seed value which specifies the above-mentioned addressee as a proper thru/or a coded data processor given in 7 any 1 terms,

An addressee specification system equipped with claim 10 which detects the addressee of this material item by predetermined incorrect detection probability by detecting the existence of the codeword in the above-mentioned material item thru/or a detection data processor given in 16 any 1 terms.

[Claim 18]

In the coded data art which generates the copy to which the water mark of an original material item was given by introducing one codeword in the group of a predetermined codeword into the copy of a material item,

The step which generates the above-mentioned codeword by generating two or more codeword multipliers,

It has the step which combines the above-mentioned codeword multiplier with the above-mentioned material item,

It is the coded data art to which each codeword of the group of the above-mentioned codeword is related with the data word which has the 1st and 2nd fields by the proper, and each value of the group of the value of these 1st and 2nd fields is expressed as the 2nd part of the above-mentioned codeword which has the 1st part of the above-mentioned codeword which has two or more 1st multipliers, and two or more 2nd multipliers.

[Claim 19]

It is the detection data-processing approach of specifying at least one codeword which exists in the version to which the water mark of a material item was given among the groups of a codeword. The version to which this water mark was given to each sample of two or more samples of the original version of this material item It is generated by combining one codeword multiplier to which it corresponds of two or more codeword multipliers. Each codeword multiplier It is related with the data word which has the 1st and 2nd fields by the proper. Each value of the group of the value of this 1st field It is expressed as the 1st part of the above-mentioned codeword which has two or more 1st multipliers. This 2nd field In the detection data-processing approach that it is expressed as the 2nd part of the above-mentioned codeword which has two or more 2nd multipliers, and each value of the 1st field of the above is expressed as a cyclic predetermined shift of two or more 1st codeword multipliers of the 1st part of the above-mentioned codeword,

The step which reproduces a codeword from the material item to which the above-

mentioned water mark was given, and generates a playback codeword,
The 1st part of the above-mentioned playback codeword is made to correlate with the 1st part of each codeword generated from the group of a codeword, and a correlation value is computed about each generated codeword,
The value of the 1st field is detected from the corresponding correlation value exceeding a predetermined threshold,
It is made to correlate with the 2nd part of each codeword generated from the group of the above-mentioned codeword of the 2nd part of the above-mentioned playback codeword, and the 2nd correlation value is computed about each generated codeword,
The detection data processor which has the step which detects the value of 1st at least one data field, and the value of 2nd at least one data field by detecting the value of the 2nd field from the 2nd corresponding correlation value exceeding a predetermined threshold.

[Claim 20]

The data signal showing the material item to which the codeword was added by claim 1 thru/or the coded data processor given in 7 any 1 terms.

[Claim 21]

Data medium with which the data signal according to claim 20 was recorded.

[Claim 22]

The computer program which offers the instruction which can be executed by computer which it is loaded [computer] to a data processor and operates this data processor as claim 1 thru/or a coded data processor given in 7 any 1 terms or claim 10 thru/or a detection data processor given in 16 any 1 terms.

[Claim 23]

The computer program which offers the instruction which can be executed by computer which it is loaded [computer] to a data processor and makes this data processor perform an approach according to claim 18 or 19.

[Claim 24]

The computer program product equipped with the medium which can be read by computer by which the information signal showing a computer program according to claim 22 or 23 is recorded.

[Claim 25]

The receiving set which combines with this input signal at least one codeword which is the receiving set which receives the signal showing a material item, is equipped with claim 1 thru/or a coded data processor given in 7 any 1 terms, and identifies an input signal to a proper.

[Claim 26]

The detection data processor or coded data processor explained below with reference to an attached drawing.

[Claim 27]

The creation approach which creates the copy to which at least one water mark of

the discernment approach of identifying at least one codeword among the predetermined codewords explained below with reference to an attached drawing, or an original material was given.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

This invention relates to the detection data processor which detects the codeword embedded at the version of a material. In some examples, a codeword is used in order to identify a material item.

[0002]

[Description of the Prior Art]

In order to identify a material, the processing which embeds information to a material is called water marking processing.

[0003]

A discernment codeword is embedded at the version of a material item, in order to identify the version of a material item. That is, the addressee of the specific version of a material can be specified by water marking processing. Here, when a material is copied or used for the intention of the distribution person of a material in a not suitable form, a distribution person can specify the version of a material from a discernment codeword, and can take a suitable cure.

[0004]

the material item which set on these specifications, and was copied or used for the intention of the feeder of a material, an owner, an implementer, or a distribution person in the not suitable form -- expedient -- the OFENDINGU item (offending item) of a material, or OFENDINGUMATE -- being real (offending material) -- it calls.

[0005]

Materials may be any of a material (information bearing material) including a video material, an audio material, an audio / video material, a software program, a digital document, and what kind of information.

[0006]

In order to make the structure of a water mark successful, it needs to be difficult for a user to remove identification code as much as possible. Moreover, it also needs to be difficult for a user to change identification code and to show others the implementer of the OFENDINGU item of a material as much as possible. An alteration as whose mask of a codeword or codeword by such user shows other users is called a KORUJON attack (collusion attack).

[0007]

[Problem(s) to be Solved by the Invention]

It is necessary to make it difficult in the structure of all water marks for the user who received the copy of the same material to succeed in a KORUJON attack. Therefore, the structure of a water mark needs to be what can specify the material item to which the water mark set as the object of a KORUJON attack is given by the high probability. this specification -- OFENDINGUMATE -- since real, it realizes by identifying the reproduced codeword. The probability (overlooking probability: false negative probability) judged as on the other hand a codeword not existing in a codeword existing must be low. Furthermore, the probability (incorrect detection probability: false positive probability) judge that is the user who performed the malfeasance accidentally [user / who has not participated in a KORUJON attack in fact] must be made as low as possible.

[0008]

U.S. Pat. No. 5664018 is indicating the water marking processing which attaches the digital water mark created from the codeword which has the multiplier of a predetermined number from a material to two or more copies. The material item to which a water mark is given is an image. The equipment which performs **** of the water mark currently indicated here changes an image into a discrete cosine transform (it is called DCT below Discrete Cosine Transform:) field. A digital water mark has normal distribution and consists of groups of a multiplier distributed at random. In a DCT field, each codeword multiplier corresponding to each DCT multiplier is added, respectively. The detailed mathematical analysis of this water marking processing for preventing an attack is indicated by July 27, 1998 which is the reference relevant to this, Jay Kilian (J. Kilian) published from MIT, EFU tea Layton (F. T. Leighton) work, and "protection (Resistance of Digital Watermarks to Collusion Attacks) of the digital water mark to a KORUJON attack."

[0009]

[Means for Solving the Problem]

The coded data processor concerning this invention generates the copy to which the water mark of an original material item was given by introducing one codeword in the group of a predetermined codeword into the copy of a material item. A coded data processor is equipped with the codeword generation machine which generates the codeword which has two or more codeword multipliers, and the coding processor which combines a codeword multiplier with a material item. Each codeword of the group of a codeword is related with the data word which has the 1st and 2nd fields by the proper. Each value of the group of the value of the 1st and 2nd fields is expressed as the 2nd part of the codeword which has the 1st part of the codeword which has two or more 1st multipliers, and two or more 2nd multipliers.

[0010]

The water mark codeword which has a hierarchical value is generable with this invention. By generating the water mark codeword which has the 1st and 2nd parts,

the data word of the 1st and 2nd fields is discriminable according to an individual. The 1st and 2nd fields can be related with different parameters, such as for example, an address parameter. For example, the distribution country of a material can be specified by the 1st field, and the domestic specific distribution ground (distribution outlet) can be specified by the 2nd field.

[0011]

In a suitable example, each value of the 1st field is expressed as a cyclic predetermined shift of two or more 1st codeword multipliers of the 1st part of a codeword. In order to realize an effective system actually, the larger possible one of the number of codewords discriminable to a proper is good. a distribution to consumer appliances, such as video equipment, the projector for movie theaters, etc. sake -- millions -- it is necessary to prepare the group of tens of millions of codewords preferably. Here, the processing which the group of the codeword which consists of 10 million codewords is generated [processing], and makes each generated codeword and a playback codeword, i.e., the 1st and 2nd fields, correlate serves as a big processing burden. By the example of this invention, the correlation value of the codeword of a lot concerning the 1st part at least can be calculated efficiently. By this example, the 1st part generates two or more 1st codeword multipliers, and is generated by [of the codeword in the group of a codeword] computing other codewords by shifting two or more 1st codeword multipliers cyclically. [at least] Thereby, the correlation value of the 1st part of all the codewords in a group is computable using Fourier transform correlator. Fourier transform correlator computes the correlation value of a lot by one processing, and mitigates an operation task substantially so that it may mention later.

[0012]

Two or more 2nd multipliers of the 2nd part of a codeword are drawn from the pseudo-random number generated using the auxiliary seed value specified with the value of the 1st field among two or more seed values. The auxiliary seed value for generating the 2nd part of a codeword may be generated by specifying the relative shift of the value of the 1st field, or two or more 1st multipliers corresponding to this. Each value of the 2nd data field is expressed as a relative shift of two or more 2nd multipliers. Hierarchical data word can be defined by constituting a water mark by the 1st and 2nd parts. Furthermore, the codeword defined by each data word is efficiently detectable using a Fourier transform correlation value while the resistance over a KORUJON attack is strong.

[0013]

In a suitable example, based on a sequence modification code, even if there are few 1st and 2nd codeword multipliers, a coding processor changes one of sequence and embeds these codeword multipliers to a material. According to this, a data processor computes a correlation value in a suitable example by returning the sequence of the 1st generated and/or the 2nd codeword multiplier, or the 1st and/or the 2nd codeword multiplier which were reproduced. Although the probability for a

KORUJON attack to be successful by shifting a codeword cyclically becomes high, this probability can be reduced by changing the sequence of a codeword multiplier.
[0014]

Furthermore, this invention offers the detection data processor defined as the attached claim. In the example of this invention, the value of the 1st and 2nd fields is specified from the 1st and 2nd parts of a water mark so that it may mention later. Preferably, this specification is realized by making two or more 1st multipliers from the version of the reproduced codeword, and the 1st part of each codeword of the group of a codeword correlate, and calculating a correlation value. This correlation is performed by Fourier transform correlator. The value of the 1st field is specified with the correlation value which is generated by Fourier transform correlator and which shows the shift of two or more 1st codeword multipliers. The 1st field specifies an auxiliary seed value and two or more 2nd codeword multipliers which constitutes the 2nd part of a water mark from this auxiliary seed value are generated. Here, the 2nd field is again pinpointed from the correlation value which shows the shift of the 2nd codeword multiplier using Fourier transform correlator.
[0015]

The further side face and the further description of this invention are defined in the attached claim.

[0016]

[Embodiment of the Invention]

A general view of a water mark system

Hereafter, the gestalt of operation of this invention is related to protection of a video image, and it explains. The number of copies is determined by the number of the users who should distribute a video image. The discernment codeword (identification code word) for identifying the copy assigned to one of these users is added to each copy.

[0017]

A video image is one example of the material protected by embedding a digital codeword. The material protected by embedding a codeword may be a material including a software program, a digital document, music, an audio signal, and what other kinds of information other than a video image.

[0018]

Drawing 1 is the block diagram showing the concrete configuration of the coded-image processor (encoding image processing apparatus) which introduces a discernment codeword into the copy of an original image. The original image I is supplied from the source and saved at a frame memory 1. This original image is copied as two or more copies to which the water mark was given (reproduce), and the discernment codeword of a proper is given to each copy. An original image is supplied to the DCT processor 2, and the DCT processor 2 divides an original image into the pixel block of 8x8, and performs DCT processing to each pixel block of 8x8. Thereby, the DCT processor 2 generates the DCT resolution picture V.

[0019]

In the following explanation, the vocabulary a "sample" shall point out the discrete sample which constitutes an image (or you may be the material of other classes in fact.). A sample may be a brightness sample of the image which can be copied also from a pixel. Therefore, vocabulary called a sample and vocabulary called a pixel may be exchangeable depending on a situation.

[0020]

The DCT image V is supplied to the coding processor (henceforth an encoder) 4. The discernment codeword is also supplied to the coding processor 4 from the discernment codeword generation machine 8.

[0021]

Two or more seed values (seed) are supplied to the discernment codeword generation machine 8. Each seed value is used in order to generate one of the discernment codewords which correspond, respectively. Each generated discernment codeword is embedded to the copy of an original image, and the image to which the water mark was given by this is generated. The discernment codeword generation machine 8 is equipped with a pseudo-random number generation machine. A pseudo-random number generation machine generates the codeword multiplier for forming a specific discernment codeword. In a desirable example, a codeword multiplier is generated based on normal distribution. In addition, it may replace with this and a codeword multiplier may be beforehand defined based on the seed value used since a pseudo-random number generation machine is initialized. Therefore, a corresponding seed value exists in each discernment codeword, and each seed value is memorized by memory 12. That is, in order to generate the discernment codeword X_i , the seed value $seed_i$ is read from memory 12, and the pseudo-random number generation machine in the discernment codeword generation machine 8 is initialized using this seed value $seed_i$.

[0022]

The DCT version of an original image is expressed in the following explanation as V. It is here,

$$V=\{v_i\}=\{v_1, v_2, v_3, v_4, \dots, v_N\}$$

It comes out, and it is and v_i is the DCT multiplier of an image. In other examples, v_i is the sampled value of an image and may express the sampled value of the image in the sampled value of an image in a space field, or other fields.

[0023]

Each discernment codeword X_i consists of codeword multipliers of n pieces as follows.

$$X_i=\{x_{ij}\}=\{x_{i1}, x_{i2}, x_{i3}, x_{i4}, \dots, x_{in}\}$$

Several n of a codeword multiplier corresponds to the measurement size of the original image V. In addition, the number of multipliers may differ and this number may be determined according to specific application.

[0024]

And the vector of the codeword multiplier which constitutes the i -th discernment codeword X_i is supplied to an encoder 4 through a channel 14. An encoder 4 generates the image W_i to which the water mark was given by adding the discernment codeword X_i to Image V . In fact, as shown in the following formulas, the image W_i to which the water mark was given is generated by applying each codeword multiplier to each multiplier of an image.

$$W_i = V + X_i$$

$$W_i = v_1 + x_{i1}, v_2 + x_{i2}, v_3 + x_{i3}, v_4 + x_{i4}, \dots, v_n + x_{in}$$

As shown in drawing 1, the image W_i to which the water mark was given is outputted by it from this image processing system, after reverse DCT conversion is carried out by the reverse DCT processor 18 which carries out reverse DCT conversion of the image generated by the encoder 4.

[0025]

Therefore, as shown in drawing 1, from an encoder 4, the group of the image to which the water mark was given is outputted. If data word is made into a maximum of 20 bits, one of the 10 million discernment codewords can be chosen, and the version W_i to which 10 million water marks were given can be generated to an original image.

[0026]

Although the copy W_i to which the water mark of Image I was given is discriminable according to an individual with this discernment codeword, in other examples, data can be sent within an image by above-mentioned 20 bits. Therefore, 20 bits of payloads of 20 bits for sending data within Image V used in order to choose a discernment codeword so that it may explain below are offered.

[0027]

The coded-image processor which is shown in drawing 1 and which generates the image to which the water mark was given is built into various products in various different scenarios with which this invention is applied. For example, a coded-image processor can be connected to a website or a web server, and the image to which the water mark was given can be downloaded. Before downloading the copy of an image, the codeword of a proper is introduced into the image to download and the codeword of this proper can detect the addressee of the downloaded image behind.

[0028]

In other examples of application, a coded-image processor is incorporated as some digital projectors (digital cinema projector), and in a movie theater, in case a discernment codeword projects a movie, it is added to an image. By this discernment codeword, the projector and movie theater which the movie projected can be pinpointed. Therefore, the projector and movie theater where the pirate edition copy was created can be pinpointed by the discernment codeword contained in the pirate edition copy which photoed the image projected from the projector and was obtained. On the other hand, the image to which the water mark was given may be copied as a photograph or printed matter, and may create and distribute the copy of the copied

photograph or printed matter. In drawing 1 , the distribution place of the image to which the water mark generated by the coded-image processor was given is shown by the distribution 19 expressed by the cloud-shaped frame.

[0029]

Detection processor

Drawing 2 is the block diagram showing the configuration of the detection image processing system (detecting image processing apparatus) which detects one or more codewords currently embedded in the OFENDINGU image (offending marked image) to which the water mark was given. Speaking comprehensively, the detection image processing system shown in drawing 2 having the function to identify one or more codewords which exist in OFENDINGU of an image, i.e., a copy.

[0030]

OFENDINGU version W' of the image to which the water mark was given is supplied from the source of data, and is saved at a frame memory 20. Since the detection processing in this detection image processing system needs the original version of an image, the original version of an image is saved at the frame memory 24. The original version of OFENDINGU version W' of the image to which the water mark was given, and an image is supplied to the registration processor (registration processor) 30 through the connection channels 26 and 28 according to individual, respectively.

[0031]

As mentioned above, OFENDINGU version W' of an image may have been generated by photoing or copying some images W_i to which the water mark was given. Then, in order to raise the detection ratio of a discernment codeword, the registration processor 30 arranges substantially the original version of the OFENDINGU image saved at frame memories 20 and 24, respectively, and an image (align). This purpose is investigating correspondence relation with the sample of the corresponding image W_i with which Sample I and the water mark of an original image are attached, and the codeword multiplier's is added.

[0032]

This registration processing is explained using drawing 3 . Drawing 3 compares OFENDINGU version W' of the original image I and the image to which the water mark was given, and is shown. As shown in drawing 3 , OFENDINGU version W' of the image to which the water mark was given has offset to the original image, and this offset may originate in the relative visual field of a camera that the OFENDINGU version of the image to which the water mark was given was generated.

[0033]


In order to reproduce the expression of a codeword multiplier, it is necessary to subtract the right sample of an original image from OFENDINGU version W' of the image to which the water mark was given. Two images are arranged for this processing. As shown in drawing 3 , registered image W'' has the boundary region (peripheral area) PA which contains in an original image the part not existing.

[0034]

By other examples, when an OFENDINGU version downloads, for example from the Internet, correspondence relation with the version I of an original image may already be in **, and, in such a case, it is not necessary to use the registration processor 30 with OFENDINGU image W'. Then, this detection image processing system is equipped with the alternative-channel 32 for supplying directly the image to which the water mark was given to the playback processor 40.

[0035]

Registered image W'' is supplied to the playback processor 40. The copy of the original image I is also supplied to the playback processor 40 through the 2nd channel 44. Image W'' and the original image I which were registered are changed into a DCT field by the DCT processor 46. Next, as shown in the following formulas, presumed codeword X' is computed by subtracting sample V' of the DCT field of the image to which the water mark was given from the sample V of the DCT field of an original image.

 ID=000003


Therefore, the playback processor 40 outputs the estimate of the multiplier of the codeword which should be identified through the connection channel 50. Reproduced codeword X' is supplied to the 1st input terminal of correlator 52. The codeword Xi generated with the codeword generation vessel 54 is supplied to the 2nd input terminal of correlator 52. The codeword generation machine 54 generates the group of all possible codewords using the predetermined seed value which identifies to a proper the codeword read from memory 58 like the above-mentioned discernment codeword generation machine 8.

[0036]

Correlator 52 generates the similar value sim of n pieces (i). In one example, the similar value sim (i) is computed by searching for the correlation based on the following formulas.

[0037]

[Equation 1]

 ID=000004

[0038]

Each of the similar value sim of n pieces (i) is supplied to a detector 60. and a detector 60 analyzes the similar value sim of n possible codewords (i) which is alike, respectively and receives. The relation between the example of the similar value sim (i) generated by correlator 52 and the threshold TH of each possible codeword is shown in drawing 4 . As shown in drawing 4 , two codewords 2001 and 12345 are over the threshold TH . For this reason, a detector 60 judges with the OFENDINGU image having been created from the version of the image to which the water mark corresponding to a codeword 2001 and a codeword 12345 was given. Therefore, in this example, the height of the threshold TH which guarantees incorrect detection probability can be set up based on the incorrect detection probability (false positive probability) determined with the magnitude of the population which is 10 million, and water mark reinforcement (watermarking strength). By the example shown in drawing 4 , when the similar value generated by correlator 52 is over the threshold, it has this incorrect detection probability, the addressee of the image to which this water mark was given performs a malfeasance, and it is judged that it participated in creation of the OFENDINGU version W_i of the image to which the water mark was given.

[0039]

Hereafter, the water mark system feature and advantage which are shown in drawing 1 and drawing 2 are explained.

[0040]

Registration

The processing which arranges the OFENDINGU version of the image to which the water mark was given, and the copy of an original image includes the processing which investigates correlation with the sample of an original image, and the sample of the image to which the water mark was given. This correlation processing is performed by shifting each sample of an image by different shift amount. This processing is explained using drawing 5 . Drawing 5 A shows the discrete sample of the original image I , and drawing 5 B shows the discrete sample of OFENDINGU image W' to which the water mark was given. As shown in drawing 5 A and drawing 5 B, the time difference between each sample is dt which becomes settled with a sampling rate. The group of each sample of these images is shifted and the result of having made the discrete sample correlating is shown in drawing 5 C.

[0041]

As shown in drawing 5 C, the correlation peak is the highest between the 6th sample and the 7th sample. Then, to an original image, only this amount is shifted and the OFENDINGU image to which the water mark was given is registered.

[0042]

Fourier decode

The water mark system mentioned above with reference to drawing 1 and drawing 2 can create the version to which 10 million water marks were given to the original image. This is realized by using the value of a 20-bit water mark. Here, in order to detect existence of the codeword in the OFENDINGU image to which the water mark was given among two or more codewords as mentioned above, it is necessary to investigate correlation with the codeword reproduced from the image, and each 10 million possible codeword. Such an operation task serves as a big processing burden.

[0043]

The correlator based on this invention shortens time amount required in order to detect the codeword in the OFENDINGU image to which the burden of this data processing was mitigated, therefore the water mark was given. This correlator based on this invention is shown in drawing 6. The correlator shown in drawing 6 offers effective technique on the alternative target to calculation of total of the correlation value mentioned above. That is, by this example, total of a correlation value is computed based on the following formulas.

$$F^{-1}[F(X')F(x(1))^{*}]$$

Here, $F(A)$ expresses the Fourier transform of A and $F^{-1}(A)$ expresses the inverse Fourier transform of A .

[0044]

The correlator 52 shown in drawing 6 is equipped with the 1st Fourier transform processor 100 and the 2nd Fourier transform processor 102. The 1st and 2nd Fourier transform processors 100 and 102 may be realized using a fast-Fourier-transform algorithm. The 2nd Fourier transform processor 102 also computes the complex conjugate $X1$ of the Fourier transform value of the generated codeword. The complex conjugate $X1$ of Fourier transform value X' of a playback codeword and the Fourier transform of the generated codeword is supplied to the 1st and 2nd input terminals of a multiplier 110, respectively. A multiplier 110 carries out the multiplication of each sample from the Fourier transform processors 100 and 102, and supplies this result to the inverse Fourier transform processor 112. From this correlator 52, the inverse Fourier transform value of the signal sample by which multiplication was carried out is outputted.

[0045]

Thus, in the correlator 52 shown in drawing 6, time amount required in order to compute correlation with n codewords X_i and playback codeword X' which were generated is shortened. This is because fast-Fourier-transform integrated circuits, such as an application-specific integrated circuit (application specific integrated circuit:ASIC) marketed, for example, can constitute the Fourier transform processors 100 and 102 and the inverse Fourier transform processor 112.

Furthermore, the inverse Fourier transform value outputted from correlator 52 offers the similar value sim of n pieces corresponding to total of the correlation value of n

pieces (i). Here, in order to use the property of the correlator 52 shown in drawing 6 , a codeword is generated by shifting one generated codeword X (1) cyclically using the specific seed value supplied to a random-number generation machine. Hereafter, generation of this codeword is explained. The 1st codeword X (1) is expressed as values x_1-x_n corresponding to the numeric value generated in pseudo-random with the codeword generation vessel 8 so that it may mention later. On the other hand, the 2nd codeword X (2) is generated by performing the cyclic shift to the 1st codeword X (1). Furthermore, as shown below, other codewords are generated by shifting the 1st codeword X (1) cyclically until the n-th codeword is shifted to the location of n-1.

$$X(1)=(x_1,x_2,x_3,x_4,\dots,x_{n-1},x_n)$$

$$X(2)=(x_2,x_3,x_4,\dots,x_{n-1},x_n,x_1)$$

$$X(3)=(x_3,x_4,\dots,x_{n-1},x_n,x_1,x_2)$$

...

$$X(n)=(x_n,x_1,x_2,x_3,x_4,\dots,x_{n-2},x_{n-1})$$

The correlator 52 which performs the Fourier transform can compute all the similar values about all n codewords by one processing by constituting a part or all of a group of a codeword that is generated by the coded-image processor using the group of this codeword. Therefore, the total sim of the similar value of n pieces (i) is generated by the shift to which it corresponds from 1 to an original codeword to n as mentioned above, and as shown in drawing 4 , the total sim of a big similar value (i) is generated about at least one codeword. Thus, correlator 52 can receive only one generated codeword corresponding to the 1st codeword X (1), and as shown in drawing 4 , it can compute the similar value about the group of n codewords.

[0046]

If the sample contained in a codeword like [it is ***** and] from the above explanation is N individual, a possible circular shift is only N individual. Therefore, if the population p of a required codeword is larger than N, the water mark used as two or more foundations is needed. The water mark used as each foundation is shifted cyclically, and the peculiar codeword of N individual is generated.

[0047]

When the image to which the water mark was given constitutes one of two or more of the images, such as for example, a video sequence, the same codeword can be given to each image. Therefore, as mentioned above, if the codeword under one judgment (suspected code word) is specified using the Fourier transform correlator shown in drawing 6 , even if it uses the total sim of all correlation values (i), the correlation value which follows is computable. What is necessary is here, to perform correlation processing only to the codeword specified by the Fourier transform correlator shown in drawing 6 , since the codeword under judgment is already specified.

[0048]

Moreover, the complex conjugate of the Fourier transform value of a playback

codeword may be computed instead of computing the complex conjugate of the Fourier transform value of the 1st generated codeword X1. This processing is expressed as the 2nd modification of processing by the Fourier transform correlator shown below.

$$F^{-1}[F(X') * F(x(1))]$$

Thus, either the complex conjugate of the Fourier transform value of a playback codeword and the Fourier transform value of the generated codeword are computed by either of the Fourier transform processors 100 and 102.

[0049]

Secret sequence modification of a codeword

There is a problem that the security of a water mark falls, by the technique of making shift the 1st codeword X1 cyclically, and generating a codeword. This is because two images to which the water mark was given are compared in a KORUJON attack. When the codeword which are two versions of the same codeword which was made to shift the same codeword cyclically and generated it is added to each image, those who try a KORUJON attack specify the difference between 2 materials to which the water mark was given, therefore it becomes easy to specify a codeword. If those who try a KORUJON attack can specify a codeword, this person can remove a water mark, or can alter a water mark, and can pretend to be the others.

[0050]

In order to prevent such a KORUJON attack, by this example, the sequence of each codeword multiplier of each codeword shifted cyclically is changed at random based on the secret sequence modification code (secret permutation code) pi. A sequence change of a codeword multiplier is made secret to the addressee of the image to which the water mark was given. It becomes difficult for those who try a KORUJON attack to specify by this correlation between two images to which the water mark was given, and possibility that a KORUJON attack will be successful falls.

[0051]

In a detection image processing system, the secret sequence exchange code pi is known. Correlation processing is performed after detection performs reverse-order exchange pi- in image-processing equipment to the codeword multiplier or playback codeword multiplier which the codeword generation machine or the playback processor 40 generated. The detection shown in the coded-image processor and drawing 2 which are shown in drawing 1 shows actuation of image-processing equipment to drawing 7 and drawing 8, respectively.

[0052]

Generation of a watermark codeword

Technique to have been improved for generating a water mark codeword is explained using drawing 9 and drawing 10. As mentioned above, the water mark codeword in the material item to which the water mark was given is efficiently detectable by shifting a codeword cyclically and generating two or more codewords using Fourier

transform correlator.

[0053]

Moreover, when the 1st codeword X_1 is shifted cyclically and a codeword is generated as mentioned above, there is a problem of becoming easy to receive the attack by KORUJON attack. Such possibility can be reduced by changing the sequence of a codeword multiplier in secret sequence modification code as mentioned above.

[0054]

In order to make still lower possibility that a KORUJON attack will be successful, in this example, the codeword generation machine 8 which operates as some coded-image processors generates the water mark codeword which has two or more parts generated according to the individual. A water mark can also be built hierarchical by generating the codeword which has two or more parts so that it may mention later. Here, a 20-bit codeword is explained in instantiation. A 20-bit codeword offers 10 million or more (1048576 pieces) codewords as a possible data value.

[0055]

A 20-bit codeword is divided into two parts which consist of 10 bits, respectively by the example explained here. This is shown in drawing 9. It is used in order to generate the 1st part [1st / the] WM1 of a 10-bit water mark. It is used in order to generate the 2nd part [2nd / the] WM2 of a 10-bit water mark. The 1st part WM1 and 2nd part WM2 are embedded in the image which should attach a water mark, as mentioned above.

[0056]

In a suitable example, the 1st part WM1 is formed by generating one codeword which consists of the 1st codeword multiplier generated with the pseudo-random number generation vessel which constitutes some codeword generation machines 8. These numeric values are generated from the basic seed value seed, as shown in drawing 9. A basic seed value may be generated from the sample of a source image.

[0057]

Each possible data value of 1024 pieces is expressed with the 1st 10-bit part WM1 of a water mark by 1024 possible shifts obtained by shifting the 1st part WM1 of the codeword generated from the basic seed value. As shown in drawing 9, this shift has the possible value of 0 to 1023.

[0058]

The 2nd part WM2 of a water mark is generated independently with the 1st part WM1 of a water mark. The shift applied to the 1st part WM1 is mapped by one of the possible auxiliary seed values (supplementary seeds) of 1024 pieces. That is, i -th shift $X_1 \rightarrow i = X_{1i}$ of a codeword specifies the auxiliary seed value (seed $_i$) of a proper. From this auxiliary seed value, the further codeword shown as X_2 in drawing 9 is generated. Thus, the relation of a predetermined proper between the seed values used in order to generate 2nd codeword X_{2i} the shift of 1st codeword X_{1i} which constitutes the 1st part WM1, and for the 2nd partial WM2 is. Here, since 1024

further possible values are expressed, the 2nd part WM2 of a water mark is shifted based on the 10-bit value of the 2nd part WM2. As shown in drawing 10 , the layered structure of a value is formed of this processing. The 1st 1024 bit generated by the 1st part WM1 offers the index of the codeword which constitutes the 2nd part WM2. The possible shift of the codeword generated from the 2nd part WM2 offers a group with a value [in the 2nd level of a layered structure / 2nd] of 1024 bits.

[0059]

By the example of this invention, the image to which the water mark was given based on two or more hierarchies can be specified. For example, since a part of country to which the image was distributed, area, or area is specified, the 1st part WM1 can be used. On the other hand, since the town and movie theater where the image to which it was given, the 2nd part, for example, water mark, of an area, was reproduced are pinpointed, a hierarchy's 2nd level can be used. The image to which the water mark was given is reproduced by this, it is more quick and the location where OFENDINGUKOPI was created from this image can be pinpointed more correctly.

[0060]

The further advantage which generates the codeword which has two parts WM1 and WM2 is [which value of the values of 1024 pieces exists in each of two hierarchy level, and] in the point which can be specified efficiently using the Fourier transform correlator shown in drawing 6 . In this combination, since the 2nd part WM2 of a water mark is generated from 1024 possible shifts of the 2nd codeword, it can specify the possible shift of the 2nd part WM2 of a codeword using the further Fourier transform decode.

[0061]

The probability for a KORUJON attack to be successful can be reduced by generating the water mark codeword which has two related parts. As mentioned above, after changing the sequence of either of the parts of these codewords, or both, you may also embed in an image.

[0062]

Other examples of application

In addition to the projector and web server which were mentioned above, the coded data processor of a water mark system is applicable to other applications. For example, this invention can receive a signal from a communication device, and can apply it also to the receiver/decoder which gives a water mark to information by introducing a codeword into this received signal. For example, a set top box receives television and a video signal from the "head end" device or multicast device of broadcast. In such an example of application, a coded data processor constitutes a part of set top box, and in case it receives and decodes a signal, it introduces a water mark codeword into a video signal. Setting in one example, this water mark codeword specifies the set top box which received and decoded the video signal as a proper.

[0063]

Furthermore, this invention is applicable also to the digital cinema receiver which receives digital cinema data (digital cinema film) from a satellite. This digital cinema receiver receives the signal showing a digital cinema, decodes this signal, and reproduces a digital cinema. This receiver is equipped with the coded data processor which introduces a water mark codeword into the decoded movie signal. A water mark codeword specifies the digital cinema receiver which received for example, digital cinema data as a proper.

[0064]

Furthermore, this invention is applicable to a digital camera or a camcorder equipped with memory and a memory controller etc. In this example of application, the coded data processor concerning this invention introduces the water mark codeword memorized by memory into the video signal photoed with the digital camera etc. In this example of application, the codeword is beforehand memorized by memory, therefore the coded data processor is not equipped with the codeword generation machine. The codeword memorized by memory is embedded under control of a memory controller at a video signal, and, thereby, specifies a video signal as a false proper target (quasi-uniquely) peculiar.

[0065]

In the further example, the coded data processor based on this invention embeds a series of water mark codewords according to an individual at each of the frame of the digital image from which the plurality which constitutes a continuous image or a continuous animation differs. These codewords may have relevance mutually and can identify now the image corresponding to each frame according to an individual by these codewords.

[0066]

The further various side faces and descriptions of this invention are defined in the attached claim. The gestalt of operation mentioned above can be changed variously, without deviating from this claim.

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of a coded-image processor.

[Drawing 2] It is the block diagram showing the configuration of a detection image processing system.

[Drawing 3] Drawing 3 A shows an original image, drawing 3 B shows the image to which the water mark was given, and drawing 3 C is drawing showing the registered image.

[Drawing 4] It is the graphical representation showing the example of the correlation result about each codeword of the group of the codeword of N individual.

[Drawing 5] Drawing 5 A is a graphical representation corresponding to the sample of the original image I, drawing 5 B is a graphical representation corresponding to image W' to which the water mark was given, and drawing 5 C is the graphical

representation showing the correlation result for every discrete sample shift of an original image and the image to which the water mark was given.

[Drawing 6] It is the block diagram showing the configuration of the correlator which is a part of detection data processor shown in drawing 2 .

[Drawing 7] It is the flow chart which shows the procedure which creates the image to which the water mark was given by the coded-image data processor.

[Drawing 8] It is the flow chart which shows the processing which specifies a water mark from the image to which the water mark which received was given by the detection data processor shown in drawing 2 .

[Drawing 9] It is drawing explaining the processing which generates the codeword multiplier which has at least two parts.

[Drawing 10] It is drawing showing the hierarchical information built using the codeword which has two parts generated by the processing shown in drawing 9 .

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the configuration of a coded-image processor.

[Drawing 2] It is the block diagram showing the configuration of a detection image processing system.

[Drawing 3] Drawing 3 A shows an original image, drawing 3 B shows the image to which the water mark was given, and drawing 3 C is drawing showing the registered image.

[Drawing 4] It is the graphical representation showing the example of the correlation result about each codeword of the group of the codeword of N individual.

[Drawing 5] Drawing 5 A is a graphical representation corresponding to the sample of the original image I, drawing 5 B is a graphical representation corresponding to image W' to which the water mark was given, and drawing 5 C is the graphical representation showing the correlation result for every discrete sample shift of an original image and the image to which the water mark was given.

[Drawing 6] It is the block diagram showing the configuration of the correlator which is a part of detection data processor shown in drawing 2 .

[Drawing 7] It is the flow chart which shows the procedure which creates the image to which the water mark was given by the coded-image data processor.

[Drawing 8] It is the flow chart which shows the processing which specifies a water mark from the image to which the water mark which received was given by the detection data processor shown in drawing 2 .

[Drawing 9] It is drawing explaining the processing which generates the codeword

multiplier which has at least two parts.

[Drawing 10] It is drawing showing the hierarchical information built using the codeword which has two parts generated by the processing shown in drawing 9 .

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-40753

(P2004-40753A)

(43) 公開日 平成16年2月5日(2004. 2. 5)

(51) Int.Cl. ⁷	F I	テーマコード(参考)
HO4N 1/387	HO4N 1/387	5B057
GO6F 17/60	GO6F 17/60 302E	5C059
GO6T 1/00	GO6F 17/60 512	5C063
GO9C 5/00	GO6T 1/00 500B	5C076
G10L 11/00	GO9C 5/00	5J104

審査請求 未請求 請求項の数 27 O L 外国語出願 (全 48 頁) 最終頁に続く

(21) 出願番号	特願2002-362515 (P2002-362515)	(71) 出願人	593081408
(22) 出願日	平成14年12月13日(2002.12.13)		ソニー・ユニテッド・キングダム・リミテッド
(31) 優先権主張番号	0129841.3		Sony United Kingdom Limited
(32) 優先日	平成13年12月13日(2001.12.13)		イギリス国 サリー, ウェーブリッジ, ブルックランズ, ザ ハイッ (番地なし)
(33) 優先権主張国	イギリス (GB)	(74) 代理人	100067736 弁理士 小池 晃
		(74) 代理人	100086335 弁理士 田村 榮一
		(74) 代理人	100096677 弁理士 伊賀 誠司

最終頁に続く

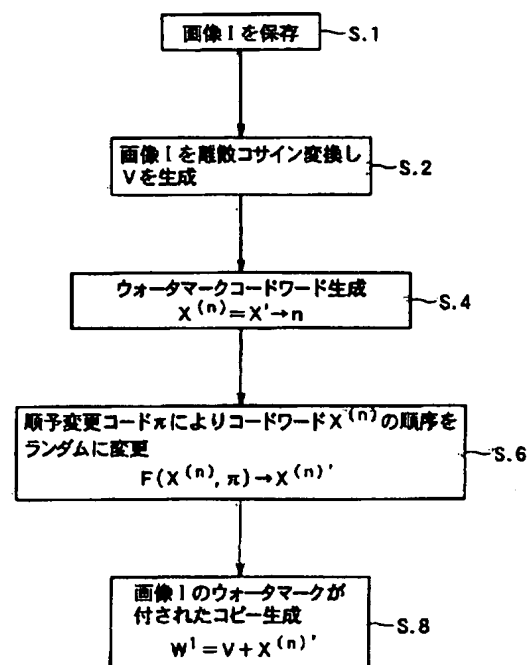
(54) 【発明の名称】 データ処理装置及びデータ処理方法

(57) 【要約】 (修正有)

【課題】 アタックに強いウォータマークシステムを提供する。

【解決手段】 マテリアルアイテムのコピーに所定のコードワードの組のうちの1つのコードワードを導入することにより、オリジナルマテリアルアイテムのウォータマークが付されたコピーを生成する符号化データ処理装置を備える。コードワードの組の各コードワードは、第1及び第2のフィールドを有するデータワードに固有に関連付けられる。第1及び第2のフィールドの値の組の各値は、第1の複数の係数を有するコードワードの第1の部分及び第2の複数の係数を有するコードワードの第2の部分として表される。第1及び第2の部分の組を有するウォータマークコードワードを生成することにより、第1及び第2のフィールドのデータワードを個別に識別できる。第1及び第2のフィールドは、例えばアドレスパラメータ等の異なるパラメータに関連付ける。

【選択図】 図7



【特許請求の範囲】

【請求項1】

マテリアルアイテムのコピーに所定のコードワードの組のうちの1つのコードワードを導入することにより、オリジナルマテリアルアイテムのウォータマークが付されたコピーを生成する符号化データ処理装置において、

複数のコードワード係数を有する上記コードワードを生成するコードワード生成器と、
上記コードワード係数を上記マテリアルアイテムに結合する符号化プロセッサとを備え、
上記コードワードの組の各コードワードは、第1及び第2のフィールドを有するデータワードに固有に関連付けられ、該第1及び第2のフィールドの値の組の各値は、第1の複数の係数を有する上記コードワードの第1の部分及び第2の複数の係数を有する上記コードワードの第2の部分として表される符号化データ処理装置。

10

【請求項2】

上記第1のフィールドの各値は、上記コードワードの第1の部分の第1の複数のコードワード係数の所定の循環的なシフトとして表されることを特徴とする請求項1記載の符号化データ処理装置。

【請求項3】

上記コードワード生成器は、上記コードワードの第1の部分が導出される疑似乱数を生成する疑似乱数生成器を備え、上記第1のフィールドの値は、上記第1のコードワード係数の所定の循環的なシフトを定義することを特徴とする請求項2記載の符号化データ処理装置。

20

【請求項4】

上記コードワードの第2の部分の第2の複数の係数は、複数のシード値のうち、上記第1のフィールドの値によって特定される補助的シード値を用いて生成された疑似乱数から導出され、該第2のフィールドの各値は、該第2の複数の係数の対応するシフトとして表されることを特徴とする請求項1乃至3いずれか1項記載の符号化データ処理装置。

【請求項5】

上記コードワード生成器は、上記マテリアルアイテムのサンプルから、上記複数のコードワード係数を生成するための第1のシード値を生成することを特徴とする請求項1乃至4いずれか1項記載の符号化データ処理装置。

【請求項6】

上記符号化プロセッサは、順序変更コードに基づいて、上記第1の複数のコードワード係数及び上記第2の複数のコードワード係数の少なくともいずれか一方の順序を変更することを特徴とする請求項1乃至5いずれか1項記載の符号化データ処理装置。

30

【請求項7】

上記マテリアルアイテムを離散コサイン変換領域に変換する離散コサイン変換プロセッサと、

上記離散コサイン変換領域のマテリアルアイテムは、複数の離散コサイン係数によって表現され、上記符号化プロセッサは、上記コードワード係数と対応する離散コサイン変換係数の1つとを加算することにより、上記コードワード係数と上記マテリアルアイテムとを結合し、該符号化プロセッサによって上記コードワードが加算された上記離散コサイン変換された画像を逆離散コサイン変換することにより、上記マテリアルアイテムのウォータマークが付されたバージョンを生成する逆離散コサイン変換プロセッサとを備える請求項6又は7記載の符号化データ処理装置。

40

【請求項8】

オーディオ信号及び画像信号のうちの少なくとも1つが供給され、複写処理の前に該オーディオ信号及び画像信号のうちの少なくとも1つにコードワードを導入する請求項1乃至7いずれか1項記載の符号化データ処理装置を備える映写装置。

【請求項9】

インターネットを介してダウンロードされるマテリアルアイテムを提供するウェブサーバであって、該マテリアルアイテムがダウンロードされる前に該マテリアルアイテムが供給

50

され、該マテリアルアイテムにコードワードを導入する請求項 1 乃至 7 いずれか 1 項記載の符号化データ処理装置を備えるウェブサーバ。

【請求項 10】

コードワードの組のうち、マテリアルアイテムのウォータマークが付されたバージョン内に存在する少なくとも 1 つのコードワードを特定する検出データ処理装置であって、該ウォータマークが付されたバージョンは、該マテリアルアイテムのオリジナルバージョンの複数のサンプルの各サンプルに、複数のコードワード係数のうちの対応する 1 つのコードワード係数を結合することにより生成され、各コードワード係数は、第 1 及び第 2 のフィールドを有するデータワードに固有に関連付けられ、該第 1 のフィールドの値の組の各値は、第 1 の複数の係数を有する上記コードワードの第 1 の部分として表され、該第 2 のフィールドは、第 2 の複数の係数を有する上記コードワードの第 2 の部分として表され、上記第 1 のフィールドの各値は、上記コードワードの第 1 の部分の第 1 の複数のコードワード係数の所定の循環的なシフトとして表されている検出データ処理装置において、上記ウォータマークが付されたマテリアルアイテムからコードワードを再生し、再生コードワードを生成する復号プロセッサと、

上記再生コードワードの第 1 の部分をコードワードの組から生成された各コードワードの第 1 の部分に相関させ、生成された各コードワードについて相関値を算出し、
所定の閾値を超える対応する相関値から第 1 のフィールドの値を検出し、
上記再生コードワードの第 2 の部分の上記コードワードの組から生成された各コードワードの第 2 の部分に相関させ、生成された各コードワードについて第 2 の相関値を算出し、
所定の閾値を超える対応する第 2 の相関値から第 2 のフィールドの値を検出することにより少なくとも 1 つの第 1 のデータフィールドの値及び少なくとも 1 つの第 2 のデータフィールドの値を検出する検出プロセッサとを備える検出データ処理装置。

【請求項 11】

上記検出プロセッサは、
上記再生コードワードの第 1 の部分に対応する部分のフーリエ変換値を算出し、
上記生成されたコードワードの第 1 の部分の第 1 の複数のコードワード係数のフーリエ変換値を算出し、
上記再生コードワードの第 1 の部分のフーリエ変換値又は上記生成されたコードワードの第 1 の部分のフーリエ変換値のいずれか一方の複素共役を算出し、
上記再生コードワードの第 1 の部分のフーリエ変換サンプルと対応する上記生成されたコードワードの第 1 の部分のフーリエ変換サンプルとを乗算して第 1 の中間積サンプルを算出し、
上記中間積サンプルを逆変換し、それぞれが上記コードワードの第 1 の部分の相関値を表す相関サンプルを算出することによって上記再生コードワードの第 1 の部分の値と上記生成された各コードワードの第 1 の部分の値との相関値を算出することを特徴とする請求項 10 記載の検出データ処理装置。

【請求項 12】

上記コードワードの第 2 の部分の第 2 の複数の係数は、複数のシード値のうち、上記第 1 のフィールドの値によって特定される補助的シード値を用いて生成された疑似乱数から導出され、該第 2 のフィールドの各値は、該第 2 の複数の係数の対応するシフトとして表され、
上記復号プロセッサは、補助的シード値の組から、上記相関値から検出された第 1 のフィールドの値によって示される補助的シード値を特定し、
上記検出プロセッサは、上記特定された補助的シード値から上記第 2 の複数のコードワード係数を生成し、上記再生コードワードの第 2 の部分に対する上記第 2 のコードワード係数のシフトから上記第 2 のデータフィールドの値を特定することを特徴とする請求項 10 又は 11 記載の検出データ処理装置。

【請求項 13】

上記検出プロセッサは、上記生成された第 2 の複数の係数を上記再生コードワードの第 2

10

20

30

40

50

の部分に相関させることにより、該再生コードワードの第2の部分に対する該生成された第2の複数の係数のシフトの値を特定することを特徴とする請求項12記載の検出データ処理装置。

【請求項14】

上記検出プロセッサは、

上記第2の部分に対応する部分のフーリエ変換値を算出し、

上記生成されたコードワードの第2の部分の第2の複数のコードワード係数のフーリエ変換値を算出し、

上記再生コードワードの第2の部分のフーリエ変換値又は上記生成されたコードワードの第2の部分のフーリエ変換値のいずれか一方の複素共役を算出し、

上記再生コードワードの第2の部分のフーリエ変換サンプルと対応する上記生成されたコードワードの第2の部分のフーリエ変換サンプルとを乗算して第2の中間積サンプルを算出し、

上記中間積サンプルを逆変換し、それぞれが上記コードワードの第2の部分の相関値を表す相関サンプルを算出することによって上記生成された第2の複数の係数を上記再生コードワードの第2の部分に相関させることを特徴とする請求項13記載の検出データ処理装置。

【請求項15】

上記第1の複数のコードワード係数及び上記第2の複数のコードワード係数の少なくともいずれか一方は、順序変更コードに基づいてマテリアルに埋め込まれ、上記複合プロセッサは、該順序変更コードに基づいて上記第1及び上記第2の再生コードワード係数の少なくともいずれか一方の順序を戻すことを特徴とする請求項10乃至14いずれか1項記載の検出データ処理装置。

【請求項16】

上記第1の複数のコードワード係数及び上記第2の複数のコードワード係数の少なくともいずれか一方は、順序変更コードに基づいてマテリアルに埋め込まれ、上記検出プロセッサは、該順序変更コードに基づいて上記第1及び第2の生成されたコードワード係数の少なくともいずれか一方の順序を戻すことを特徴とする請求項10乃至14いずれか1項記載の検出データ処理装置。

【請求項17】

マテリアルアイテムの受信者を特定する受信者特定システムにおいて、

上記受信者を固有に特定するシード値から生成されたコードワードをマテリアルアイテムに導入することにより、ウォータマークが付されたマテリアルアイテムを生成する請求項1乃至7いずれか1項記載の符号化データ処理装置と、

上記マテリアルアイテムにおけるコードワードの有無を検出することにより、所定の誤検出確率で該マテリアルアイテムの受信者を検出する請求項10乃至16いずれか1項記載の検出データ処理装置とを備える受信者特定システム。

【請求項18】

マテリアルアイテムのコピーに所定のコードワードの組のうちの1つのコードワードを導入することにより、オリジナルマテリアルアイテムのウォータマークが付されたコピーを生成する符号化データ処理方法において、

複数のコードワード係数を生成することにより上記コードワードを生成するステップと、

上記コードワード係数を上記マテリアルアイテムに結合するステップとを有し、

上記コードワードの組の各コードワードは、第1及び第2のフィールドを有するデータワードに固有に関連付けられ、該第1及び第2のフィールドの値の組の各値は、第1の複数の係数を有する上記コードワードの第1の部分及び第2の複数の係数を有する上記コードワードの第2の部分として表される符号化データ処理方法。

【請求項19】

コードワードの組のうち、マテリアルアイテムのウォータマークが付されたバージョン内に存在する少なくとも1つのコードワードを特定する検出データ処理方法であって、該ウ

10

20

30

40

50

ウォーターマークが付されたバージョンは、該マテリアルアイテムのオリジナルバージョンの複数のサンプルの各サンプルに、複数のコードワード係数のうちの対応する1つのコードワード係数を結合することにより生成され、各コードワード係数は、第1及び第2のフィールドを有するデータワードに固有に関連付けられ、該第1のフィールドの値の組の各値は、第1の複数の係数を有する上記コードワードの第1の部分として表され、該第2のフィールドは、第2の複数の係数を有する上記コードワードの第2の部分として表され、上記第1のフィールドの各値は、上記コードワードの第1の部分の第1の複数のコードワード係数の所定の循環的なシフトとして表されている検出データ処理方法において、上記ウォーターマークが付されたマテリアルアイテムからコードワードを再生し、再生コードワードを生成するステップと、

10

上記再生コードワードの第1の部分をコードワードの組から生成された各コードワードの第1の部分に相関させ、生成された各コードワードについて相関値を算出し、所定の閾値を超える対応する相関値から第1のフィールドの値を検出し、上記再生コードワードの第2の部分の上記コードワードの組から生成された各コードワードの第2の部分に相関させ、生成された各コードワードについて第2の相関値を算出し、所定の閾値を超える対応する第2の相関値から第2のフィールドの値を検出することにより少なくとも1つの第1のデータフィールドの値及び少なくとも1つの第2のデータフィールドの値を検出するステップとを有する検出データ処理装置。

【請求項20】

請求項1乃至7いずれか1項記載の符号化データ処理装置によってコードワードが付加されたマテリアルアイテムを表すデータ信号。

20

【請求項21】

請求項20記載のデータ信号が記録されたデータ媒体。

【請求項22】

データプロセッサにロードされて、該データプロセッサを請求項1乃至7いずれか1項記載の符号化データ処理装置又は請求項10乃至16いずれか1項記載の検出データ処理装置として動作させるコンピュータにより実行可能な命令を提供するコンピュータプログラム。

【請求項23】

データプロセッサにロードされて、該データプロセッサに請求項18又は19記載の方法を実行させるコンピュータにより実行可能な命令を提供するコンピュータプログラム。

30

【請求項24】

請求項22又は23記載のコンピュータプログラムを表す情報信号が記録されているコンピュータにより読取可能な媒体を備えるコンピュータプログラム製品。

【請求項25】

マテリアルアイテムを表す信号を受信する受信装置であって、請求項1乃至7いずれか1項記載の符号化データ処理装置を備え、受信信号を固有に識別する少なくとも1つのコードワードを該受信信号に結合する受信装置。

【請求項26】

添付の図面を参照して以下に説明する検出データ処理装置又は符号化データ処理装置。

40

【請求項27】

添付の図面を参照して以下に説明する所定のコードワードのうち少なくとも1つのコードワードを識別する識別方法又はオリジナルマテリアルの少なくとも1つのウォーターマークが付されたコピーを作成する作成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、マテリアルのバージョンに埋め込まれたコードワードを検出する検出データ処理装置に関する。いくつかの具体例においては、コードワードは、マテリアルアイテムを識別するために使用される。

50

【0002】

【従来の技術】

マテリアルを識別するために、マテリアルに情報を埋め込む処理は、ウォータマーキング処理と呼ばれる。

【0003】

識別コードワードは、マテリアルアイテムのバージョンを識別するために、マテリアルアイテムのバージョンに埋め込まれる。すなわち、ウォータマーキング処理により、マテリアルの特定のバージョンの受信者を特定することができる。ここで、マテリアルの配信者の意向にそぐわない形でマテリアルがコピー又は使用された場合、配信者は、識別コードワードからマテリアルのバージョンを特定し、適切な対策を講ずることができる。

10

【0004】

この明細書においては、マテリアルの供給者、所有者、作成者又は配信者の意向にそぐわない形でコピー又は使用されたマテリアルアイテムを、便宜的にマテリアルのオフエンディングアイテム (offending item) 又はオフエンディングマテリアル (offending material) と呼ぶ。

【0005】

マテリアルは、ビデオマテリアル、オーディオマテリアル、オーディオ/ビデオマテリアル、ソフトウェアプログラム、デジタル文書及びいかなる種類の情報を含むマテリアル (information bearing material) のいずれであってもよい。

20

【0006】

ウォータマークの仕組みを成功させるためには、ユーザが識別コードを除去することが可能な限り困難である必要がある。また、ユーザが識別コードを変更し、マテリアルのオフエンディングアイテムの作成者を他人にみせかけることも可能な限り困難である必要がある。このようなユーザによるコードワードのマスク又はコードワードが他のユーザを示すようにするような改竄は、コルージョンアタック (collusion attack) と呼ばれる。

【0007】

【発明が解決しようとする課題】

全てのウォータマークの仕組みにおいて、同じマテリアルのコピーを受け取ったユーザがコルージョンアタックに成功することが困難となるようにする必要がある。したがって、ウォータマークの仕組みは、コルージョンアタックの対象となったウォータマークが付されているマテリアルアイテムを高い確率で特定できるものである必要がある。この特定は、オフエンディングマテリアルから再生されたコードワードを識別することにより実現される。一方、コードワードが存在するのにコードワードが存在しないと判定してしまう確率 (見逃し確率: false negative probability) は、低くなくてはならない。更に、実際にはコルージョンアタックに加担していないユーザを誤って不正行為を行ったユーザであると判定してしまう確率 (誤検出確率: false positive probability) は、可能な限り低くしなくてはならない。

30

【0008】

米国特許第5664018号は、マテリアルから複数のコピーに所定数の係数を有するコードワードから作成されたデジタルウォータマークを付すウォータマーキング処理を開示している。ウォータマークが付されるマテリアルアイテムは、例えば画像である。ここで開示されているウォータマークの埋込を行う装置は、画像を離散コサイン変換 (Discrete Cosine Transform: 以下、DCTという。) 領域に変換する。デジタルウォータマークは、正規分布を有し、ランダムに分布した係数の組から構成されている。DCT領域において、それぞれ各DCT係数に対応する各コードワード係数が付加される。これに関連する文献である1998年7月27日、MITから発行された、ジェイ・キリアン (J. Kilian)、エフ・ティー・レイトン (F. T. Leighton) 著、「コルージョンアタックに対するデジタルウォータマークの保護 (Resi

40

50

stance of Digital Watermarks to Collusion Attacks)」には、アタックを防ぐためのこのウォータマーキング処理の詳細な数学的解析が開示されている。

【0009】

【課題を解決するための手段】

本発明に係る符号化データ処理装置は、マテリアルアイテムのコピーに所定のコードワードの組のうちの1つのコードワードを導入することにより、オリジナルマテリアルアイテムのウォータマークが付されたコピーを生成する。符号化データ処理装置は、複数のコードワード係数を有するコードワードを生成するコードワード生成器と、コードワード係数をマテリアルアイテムに結合する符号化プロセッサとを備える。コードワードの組の各コードワードは、第1及び第2のフィールドを有するデータワードに固有に関連付けられる。第1及び第2のフィールドの値の組の各値は、第1の複数の係数を有するコードワードの第1の部分及び第2の複数の係数を有するコードワードの第2の部分として表される。

【0010】

本発明により、階層的な値を有するウォータマークコードワードを生成できる。第1及び第2の部分の値を有するウォータマークコードワードを生成することにより、第1及び第2のフィールドのデータワードを個別に識別できる。第1及び第2のフィールドは、例えばアドレスパラメータ等の異なるパラメータに関連付けることができる。例えば、第1のフィールドによりマテリアルの配信国を特定し、第2のフィールドにより、その国内の特定の配信地(distribution outlet)を特定することができる。

【0011】

好適な具体例においては、第1のフィールドの各値は、コードワードの第1の部分の第1の複数のコードワード係数の所定の循環的なシフトとして表される。現実的に有効なシステムを実現するためには、固有に識別できるコードワードの数は可能な限り大きい方がよい。例えばビデオ機器等の民生用機器や映画館用の映写機等への配信のためには、数百万、好ましくは数千万のコードワードの組を設ける必要がある。ここで、一千万個のコードワードからなるコードワードの組を生成し、生成された各コードワードと再生コードワード、すなわち第1及び第2のフィールドとを相関させる処理は、大きな処理負担となる。本発明の具体例では、一組のコードワードの少なくとも第1の部分に関する相関値の演算を効率的に行うことができる。この具体例では、コードワードの組内のコードワードの少なくとも第1の部分は、第1の複数のコードワード係数を生成し、第1の複数のコードワード係数を循環的にシフトして他のコードワードを算出することにより生成される。これにより、組内の全てのコードワードの第1の部分の相関値は、フーリエ変換相関器を用いて算出できる。後述するように、フーリエ変換相関器は、一組の相関値を1回の処理で算出し、演算タスクを実質的に軽減する。

【0012】

コードワードの第2の部分の第2の複数の係数は、複数のシード値のうち、第1のフィールドの値によって特定される補助的シード値を用いて生成された疑似乱数から導出される。コードワードの第2の部分の値を生成するための補助的シード値は、第1のフィールドの値又はこれに対応する第1の複数の係数の相対的シフトを特定することにより生成してもよい。第2のデータフィールドの各値は、第2の複数の係数の相対的なシフトとして表される。ウォータマークを第1及び第2の部分により構成することにより、階層的なデータワードを定義できる。更に、各データワードによって定義されるコードワードは、コルジョンアタックに対する耐性が強いとともに、フーリエ変換相関値を用いて効率的に検出できる。

【0013】

好適な具体例においては、符号化プロセッサは、順序変更コードに基づいて、第1及び第2のコードワード係数の少なくともいずれか一方の順序を変更してこれらのコードワード係数をマテリアルに埋め込む。これに応じて、好適な具体例においては、データプロセッサは、生成された第1の及び／又は第2のコードワード係数又は再生された第1の及び／

又は第2のコードワード係数の順序を戻して相関値を算出する。コードワードを循環的にシフトすることによりコルジョニアタックが成功する確率が高くなるが、コードワード係数の順序を変更することにより、この確率を低減することができる。

【0014】

更に、本発明は、添付の請求の範囲に定義されている検出データ処理装置を提供する。後述するように、本発明の具体例においては、ウォータマークの第1及び第2の部分から第1及び第2のフィールドの値を特定する。好ましくは、この特定は、再生されたコードワードのバージョンからの第1の複数の係数と、コードワードの組の各コードワードの第1の部分とを相関させて相関値を求めることにより実現される。この相関は、フーリエ変換相関器により行われる。第1のフィールドの値は、フーリエ変換相関器により生成される、第1の複数のコードワード係数のシフトを示す相関値によって特定される。第1のフィールドは、補助的シード値を特定し、この補助的シード値からウォータマークの第2の部分構成する第2の複数のコードワード係数が生成されている。ここで、再びフーリエ変換相関器を用いて、第2のコードワード係数のシフトを示す相関値から第2のフィールドが特定される。

【0015】

本発明の更なる側面及び特徴は、添付の請求の範囲において定義されている。

【0016】

【発明の実施の形態】

ウォータマークシステムの概観

以下、本発明の実施の形態をビデオ画像の保護に関連させて説明する。ビデオ画像を配信すべきユーザの数によりコピーの数が決定する。各コピーには、これらのユーザのうちの1人に割り当てられたコピーを識別するための識別コードワード (identification code word) が付加される。

【0017】

ビデオ画像は、デジタルコードワードを埋め込むことにより保護されるマテリアルの一具体例である。コードワードを埋め込むことにより保護されるマテリアルは、ビデオ画像の他に、ソフトウェアプログラム、デジタル文書、音楽、オーディオ信号及び他のいかなる種類の情報を含むマテリアルであってもよい。

【0018】

図1は、オリジナル画像のコピーに識別コードワードを導入する符号化画像処理装置 (encoding image processing apparatus) の具体的構成を示すブロック図である。オリジナル画像Iは、ソースから供給され、フレームメモリ1に保存される。このオリジナル画像は、ウォータマークが付された複数のコピーとして複製される (reproduce) ものであり、各コピーには、固有の識別コードワードが付される。オリジナル画像は、DCTプロセッサ2に供給され、DCTプロセッサ2は、オリジナル画像を8×8の画素ブロックに分割し、8×8の各画素ブロックにDCT処理を施す。これにより、DCTプロセッサ2は、DCT変換画像Vを生成する。

【0019】

以下の説明において、「サンプル」という用語は、画像 (又は、実際には他の種類のマテリアルであってもよい。) を構成する離散サンプルを指すものとする。サンプルは、画素からも複製することができる画像の輝度サンプルであってもよい。したがって、サンプルという用語と画素という用語は、状況によっては交換可能である場合もある。

【0020】

DCT画像Vは、符号化プロセッサ (以下、エンコーダともいう。) 4に供給される。符号化プロセッサ4には、識別コードワード生成器8から識別コードワードも供給されている。

【0021】

識別コードワード生成器8には、複数のシード値 (seed) が供給される。各シード値は、それぞれ対応する識別コードワードの1つを生成するために使用される。生成された

10

20

30

40

50

各識別コードワードは、オリジナル画像のコピーに埋め込まれ、これによりウォーターマークが付された画像が生成される。識別コードワード生成器8は、疑似乱数生成器を備える。疑似乱数生成器は、特定の識別コードワードを形成するためのコードワード係数を生成する。好ましい具体例においては、コードワード係数は、正規分布に基づいて生成される。なお、これに代えて、コードワード係数は、疑似乱数生成器を初期化するために用いるシード値に基づいて、予め定めてもよい。したがって、各識別コードワードには、対応するシード値が存在し、各シード値は、メモリ12に記憶されている。すなわち、識別コードワード X_i を生成するために、シード値 $seed_i$ をメモリ12から読み出し、このシード値 $seed_i$ を用いて、識別コードワード生成器8内の疑似乱数生成器を初期化する。

10

【0022】

以下の説明では、オリジナル画像のDCTバージョンを V と表す。ここで、

$$V = \{v_i\} = \{v_1, v_2, v_3, v_4, \dots, v_N\}$$

であり、 v_i は、画像のDCT係数である。他の具体例においては、 v_i は、画像のサンプル値であり、空間領域における画像のサンプル値又は他の領域における画像のサンプル値を表すものであってもよい。

【0023】

各識別コードワード X_i は、以下のように、 n 個のコードワード係数から構成されている。

$$X_i = \{x_{ij}\} = \{x_{i1}, x_{i2}, x_{i3}, x_{i4}, \dots, x_{in}\}$$

20

コードワード係数の数 n は、オリジナル画像 V のサンプル数に対応する。なお、係数の数は異なるものであってもよく、この数は、特定のアプリケーションに応じて決定してもよい。

【0024】

そして、 i 番目の識別コードワード X_i を構成するコードワード係数のベクトルは、チャンネル14を介してエンコーダ4に供給される。エンコーダ4は、画像 V に識別コードワード X_i を付加することにより、ウォーターマークが付された画像 W_i を生成する。実際には、以下の式に示すように、画像の各係数に各コードワード係数を加えることにより、ウォーターマークが付された画像 W_i が生成される。

$$W_i = V + X_i$$

30

$$W_i = v_1 + x_{i1}, v_2 + x_{i2}, v_3 + x_{i3}, v_4 + x_{i4}, \dots, v_n + x_{in}$$

図1に示すように、ウォーターマークが付された画像 W_i は、エンコーダ4により生成された画像を逆DCT変換する逆DCTプロセッサ18によって、逆DCT変換された後、この画像処理装置から出力される。

【0025】

したがって、図1に示すように、エンコーダ4からは、ウォーターマークが付された画像の組が出力される。データワードを最大20ビットとすると、一千万個の識別コードワードの1つを選択することができ、オリジナル画像に対して、一千万個のウォーターマークが付されたバージョン W_i を生成することができる。

40

【0026】

この識別コードワードにより、画像 I のウォーターマークが付されたコピー W_i を個別に識別することができるが、他の具体例においては、上述の20ビットにより、画像内でデータを送ることができる。したがって、以下に説明するように、識別コードワードを選択するために使用される20ビットは、画像 V 内でデータを送るための20ビットのパイロードを提供する。

【0027】

図1に示す、ウォーターマークが付された画像を生成する符号化画像処理装置は、本発明が適用される様々な異なるシナリオにおいて、様々な製品に組み込まれる。例えば、符号化画像処理装置をウェブサイト又はウェブサーバに接続して、ウォーターマークが付された画

50

像をダウンロードすることができる。画像のコピーをダウンロードする前に、ダウンロードされる画像には固有のコードワードが導入され、この固有のコードワードにより、ダウンロードされた画像の受信者を後に検出することができる。

【0028】

他の適用例では、符号化画像処理装置は、デジタル映写機 (digital cinema projector) の一部として組み込まれ、識別コードワードは、例えば映画館において、映画を映写する際に、映像に付加される。この識別コードワードにより、映画が映写された映写機及び映画館を特定することができる。したがって、映写機から映写された映像を撮影して得られた海賊版コピーに含まれる識別コードワードにより、その海賊版コピーが作成された映写機及び映画館を特定することができる。一方、ウォーターマークが付された画像は、写真又は印刷物として複写されてもよく、複写された写真又は印刷物のコピーを作成及び配布してもよい。図1においては、符号化画像処理装置によって生成されるウォーターマークが付された画像の配信先は、雲形の枠で表現された配信19で示されている。

【0029】

検出プロセッサ

図2は、ウォーターマークが付されたオフエンディング画像 (offending marked image) 内に埋め込まれている1つ以上のコードワードを検出する検出画像処理装置 (detecting image processing apparatus) の構成を示すブロック図である。包括的にいえば、図2に示す検出画像処理装置は、画像のオフエンディング、すなわちコピー内に存在する1つ以上のコードワードを識別する機能を有している。

【0030】

ウォーターマークが付された画像のオフエンディングバージョンW' は、データ源から供給され、フレームメモリ20に保存される。この検出画像処理装置における検出処理は、画像のオリジナルバージョンを必要とするため、フレームメモリ24には、画像のオリジナルバージョンが保存されている。ウォーターマークが付された画像のオフエンディングバージョンW' 及び画像のオリジナルバージョンは、それぞれ個別の接続チャンネル26、28を介して、登録プロセッサ (registration processor) 30に供給される。

【0031】

上述のように、画像のオフエンディングバージョンW' は、ウォーターマークが付された画像W iの一部を撮影又は複写することにより生成された可能性がある。そこで、識別コードワードの検出率を高めるために、登録プロセッサ30は、それぞれフレームメモリ20、24に保存されているオフエンディング画像と画像のオリジナルバージョンとを実質的に揃える (align)。この目的は、オリジナル画像のサンプルIと、ウォーターマークが付され、コードワード係数が付加されている対応する画像W iのサンプルとの対応関係を調べることである。

【0032】

この登録処理を図3を用いて説明する。図3は、オリジナル画像Iとウォーターマークが付された画像のオフエンディングバージョンW' とを比較して示している。図3に示すように、ウォーターマークが付された画像のオフエンディングバージョンW' は、オリジナル画像に対してオフセットを有しており、このオフセットは、ウォーターマークが付された画像のオフエンディングバージョンが生成されたカメラの相対的な視野に起因する可能性がある。

【0033】

コードワード係数の表現を再生するために、ウォーターマークが付された画像のオフエンディングバージョンW' からオリジナル画像の正しいサンプルを減算する必要がある。この処理のために、2つの画像が揃えられる。図3に示すように、登録された画像W'' は、オリジナル画像には存在しない部分を含む周辺領域 (peripheral area) P

10

20

30

40

50

Aを有している。

【0034】

他の具体例では、例えばインターネットからオフエンディングバージョンがダウンロードされた場合等、オフエンディング画像W'と既にオリジナル画像のバージョンIとの対応関係が明かであることがあり、このような場合、登録プロセッサ30を使用する必要はない。そこで、この検出画像処理装置は、ウォーターマークが付された画像を再生プロセッサ40に直接供給するための代替的なチャンネル32を備えている。

【0035】

登録された画像W''は、再生プロセッサ40に供給される。再生プロセッサ40には、第2のチャンネル44を介して、オリジナル画像Iのコピーも供給される。登録された画像W''及びオリジナル画像Iは、DCTプロセッサ46によって、DCT領域に変換される。次に、以下の式に示すように、オリジナル画像のDCT領域のサンプルVからウォーターマークが付された画像のDCT領域のサンプルV'を減算することにより、推定コードワードX'が算出される。

$$X' = V' - V$$

$$= v'1 - v1, v'2 - v2, v'3 - v3, v'4 - v4, \dots, v$$

$$n - v_n$$

$$= x'1, x'2, x'3, x'4, \dots, x'n$$

したがって、再生プロセッサ40は、接続チャンネル50を介して、識別すべきコードワードの係数の推定値を出力する。再生されたコードワードX'は、相関器52の第1の入力端子に供給される。相関器52の第2の入力端子には、コードワード生成器54によって生成されたコードワードXiが供給されている。コードワード生成器54は、上述の識別コードワード生成器8と同様に、メモリ58から読み出したコードワードを固有に識別する所定のシード値を用いて全ての可能なコードワードの組を生成する。

【0036】

相関器52は、n個の類似値sim(i)を生成する。一具体例においては、類似値sim(i)は、以下の式に基づく相関を求めることにより算出される。

【0037】

【数1】

$$sim(i) = \frac{X^i * X'}{\sqrt{X^i * X'}} = \frac{x^i_1 * x'_1 + x^i_2 * x'_2 + x^i_3 * x'_3 + \dots + x^i_n * x'_n}{\sqrt{x^i_1 * x'_1 + x^i_2 * x'_2 + x^i_3 * x'_3 + \dots + x^i_n * x'_n}}$$

【0038】

n個の類似値sim(i)のそれぞれは、検出器60に供給される。そして、検出器60は、n個の可能なコードワードのそれぞれに対する類似値sim(i)を分析する。相関器52によって生成される類似値sim(i)の具体例と、可能な各コードワードの閾値THとの関係を図4に示す。図4に示すように、2つのコードワード2001、12345が閾値THを超えている。このため、検出器60は、コードワード2001及びコードワード12345に対応するウォーターマークが付された画像のバージョンからオフエンディング画像が作成されたと判定する。したがって、この具体例においては、一千万である母集団の大きさにより決定される誤検出確率(false positive probability)と、ウォーターマーク強度(watermarking strength)とに基づいて、誤検出確率を保証する閾値THの高さを設定することができる。図4に示す具体例では、相関器52によって生成された類似値が閾値を超えている場合、この誤検出確率をもって、このウォーターマークが付された画像の受信者が不正行為を行い、ウ

10

20

30

40

50

ウォーターマークが付された画像のオフエンディングバージョン W_i の作成に関与したと判断される。

【0039】

以下、図1及び図2に示すウォーターマークシステムの特徴及び利点を説明する。

【0040】

登録

ウォーターマークが付された画像のオフエンディングバージョンと、オリジナル画像のコピーとを揃える処理は、オリジナル画像のサンプルと、ウォーターマークが付された画像のサンプルとの相関を調べる処理を含む。この相関処理は、画像の各サンプルを異なるシフト量でシフトさせて実行される。この処理を図5を用いて説明する。図5Aは、オリジナル画像 I の離散サンプルを示し、図5Bは、ウォーターマークが付されたオフエンディング画像 W' の離散サンプルを示している。図5A及び図5Bに示すように、各サンプル間の時間差は、サンプリングレートにより定まる dt である。これらの画像の各サンプルの組をシフトし、離散サンプルを相関させた結果を図5Cに示す。

【0041】

図5Cに示すように、第6サンプルと第7サンプルの間で相関ピークが最高になっている。そこで、ウォーターマークが付されたオフエンディング画像は、オリジナル画像に対してこの量だけシフトされて登録される。

【0042】

フーリエ復号

図1及び図2を参照して上述したウォーターマークシステムは、オリジナル画像に対して一千万個のウォーターマークが付されたバージョンを作成することができる。これは、20ビットのウォーターマークの値を用いることにより実現される。ここで、上述のように、複数のコードワードのうち、ウォーターマークが付されたオフエンディング画像内のコードワードの存在を検出するためには、その画像から再生されたコードワードと、一千万個の可能な各コードワードとの相関を調べる必要がある。このような演算タスクは大きな処理負担となる。

【0043】

本発明に基づく相関器は、この演算処理の負担を軽減し、したがってウォーターマークが付されたオフエンディング画像内のコードワードを検出するために必要な時間を短縮する。本発明に基づくこの相関器を図6に示す。図6に示す相関器は、上述した相関値の総和の算出に対する代替的で有効な手法を提供する。すなわち、この具体例では、相関値の総和は、以下の式に基づいて算出される。

$$F^{-1} [F(X') F(x(1)) *]$$

ここで、 $F(A)$ は A のフーリエ変換を表し、 $F^{-1}(A)$ は A の逆フーリエ変換を表す。

【0044】

図6に示す相関器52は、第1のフーリエ変換プロセッサ100と、第2のフーリエ変換プロセッサ102とを備える。第1及び第2のフーリエ変換プロセッサ100、102は、高速フーリエ変換アルゴリズムを用いて実現してもよい。第2のフーリエ変換プロセッサ102は、生成されたコードワードのフーリエ変換値の複素共役 X_1 も算出する。再生コードワードのフーリエ変換値 X' と、生成されたコードワードのフーリエ変換の複素共役 X_1 は、それぞれ乗算器110の第1及び第2の入力端子に供給される。乗算器110は、フーリエ変換プロセッサ100、102からの各サンプルを乗算し、この結果を逆フーリエ変換プロセッサ112に供給する。この相関器52からは、乗算された信号サンプルの逆フーリエ変換値が出力される。

【0045】

このように、図6に示す相関器52では、生成された n 個のコードワード X_i と再生コードワード X' との相関を算出するために必要な時間が短縮される。これは、フーリエ変換プロセッサ100、102及び逆フーリエ変換プロセッサ112を例えば市販されている

特定用途向け集積回路 (application specific integrated circuit: ASIC) 等の高速フーリエ変換集積回路により構成できるためである。更に、相関器 52 から出力される逆フーリエ変換値は、 n 個の相関値の総和に対応する n 個の類似値 $\text{sim}(i)$ を提供する。ここで、図 6 に示す相関器 52 の特性を利用するために、コードワードは、乱数生成器に供給される特定のシード値を用いて、生成された 1 つのコードワード $X(1)$ を循環的にシフトすることにより生成される。以下、このコードワードの生成について説明する。後述するように、第 1 のコードワード $X(1)$ は、コードワード生成器 8 によって疑似ランダム的に生成された数値に対応する値 $x_1 \sim x_n$ として表される。一方、第 2 のコードワード $X(2)$ は、第 1 のコードワード $X(1)$ に対する循環的シフトを実行することにより生成される。更に、以下に示すように、この他のコードワードは、 n 番目のコードワードが $n-1$ の位置にシフトされるまで、第 1 のコードワード $X(1)$ を循環的にシフトすることにより生成される。

$X(1) = (x_1, x_2, x_3, x_4, \dots, x_{n-1}, x_n)$

$X(2) = (x_2, x_3, x_4, \dots, x_{n-1}, x_n, x_1)$

$X(3) = (x_3, x_4, \dots, x_{n-1}, x_n, x_1, x_2)$

...

$X(n) = (x_n, x_1, x_2, x_3, x_4, \dots, x_{n-2}, x_{n-1})$

このコードワードの組を用いて、符号化画像プロセッサによって生成されるコードワードの組の一部又は全部を構成することにより、フーリエ変換を行う相関器 52 は、一回の処理で n 個の全てのコードワードに関する全ての類似値を算出することができる。したがって、上述のように、オリジナルのコードワードに対する 1 から n までの対応するシフトにより、 n 個の類似値の総和 $\text{sim}(i)$ が生成され、図 4 に示すように、少なくとも 1 つのコードワードについて、大きな類似値の総和 $\text{sim}(i)$ が生成される。このように、相関器 52 は、第 1 のコードワード $X(1)$ に対応する 1 つの生成されたコードワードのみを受け取って、図 4 に示すように n 個のコードワードの組に関する類似値を算出することができる。

【0046】

以上の説明から明かなように、コードワードに含まれるサンプルが N 個であれば、可能な循環シフトは N 個のみである。したがって、必要なコードワードの母集団 p が N より大きければ、複数の基礎となるウォータマークが必要となる。各基礎となるウォータマークは、循環的にシフトされ、 N 個の固有なコードワードが生成される。

【0047】

ウォータマークが付された画像が、例えばビデオシーケンス等の複数の画像の 1 つを構成する場合、各画像には同じコードワードを付すことができる。したがって、図 6 に示すフーリエ変換相関器を用いて、1 つの判定中のコードワード (suspected code word) が特定されると、上述のように、全ての相関値の総和 $\text{sim}(i)$ を用いても、後続する相関値を算出することができる。ここで、判定中のコードワードは既に特定されているため、相関処理は、図 6 に示すフーリエ変換相関器によって特定されたコードワードに対してのみ行えばよい。

【0048】

また、生成された第 1 のコードワード X_1 のフーリエ変換値の複素共役を算出する代わりに、再生コードワードのフーリエ変換値の複素共役を算出してもよい。この処理は、以下に示すフーリエ変換相関器による処理の第 2 の変形例として表される。

$F^{-1} [F(X') * F(x(1))]$

このように、再生コードワードのフーリエ変換値の複素共役及び生成されたコードワードのフーリエ変換値のいずれかがフーリエ変換プロセッサ 100、102 のいずれかによって算出される。

【0049】

コードワードの秘密の順序変更

第 1 のコードワード X_1 を循環的にシフトさせてコードワードを生成する手法では、ウォ

ータマークのセキュリティが低下するという問題がある。これは、コルージョンアタックにおいては、ウォータマークが付された2つの画像が比較されるからである。各画像に対し、同じコードワードを循環的にシフトさせて生成した同じコードワードの2つのバージョンであるコードワードを付加した場合、コルージョンアタックを試みる者は、ウォータマークが付された2マテリアル間の相異を特定し、したがってコードワードを特定しやすくなる。コルージョンアタックを試みる者がコードワードを特定できると、この者は、ウォータマークを除去し、又はウォータマークを改竄して他者を装うことができるようになる。

【0050】

このようなコルージョンアタックを防止するために、この具体例では、秘密の順序変更コード (secret permutation code) π に基づいて、循環的にシフトされた各コードワードの各コードワード係数の順序をランダムに変更する。コードワード係数の順序変更は、ウォータマークが付された画像の受信者に対して秘密にされる。これにより、コルージョンアタックを試みる者がウォータマークが付された2つの画像間の相関を特定することが困難になり、コルージョンアタックが成功する可能性が低下する。

【0051】

検出画像処理装置においては、秘密の順序入替コード π は既知である。検出が像処理装置においては、コードワード生成器又は再生プロセッサ40が生成したコードワード係数又は再生コードワード係数に対して逆の順序入替 π^{-1} を実行した後、相関処理を行う。図1に示す符号化画像処理装置及び図2に示す検出が像処理装置の動作をそれぞれ図7及び図8に示す。

【0052】

ウォータマークコードワードの生成

ウォータマークコードワードを生成するための改善された手法について、図9及び図10を用いて説明する。上述のように、コードワードを循環的にシフトさせて複数のコードワードを生成することにより、フーリエ変換相関器を用いて、ウォータマークが付されたマテリアルアイテム内のウォータマークコードワードを効率的に検出することができる。

【0053】

また、上述のように、第1のコードワード X_1 を循環的にシフトさせてコードワードを生成すると、コルージョンアタックによる攻撃を受けやすくなるという問題がある。このような可能性は、上述のように、秘密の順序変更コードでコードワード係数の順序を変更することにより低減できる。

【0054】

コルージョンアタックが成功する可能性を更に低くするために、この具体例においては、符号化画像処理装置の一部として動作するコードワード生成器8は、個別に生成された複数の部分を有するウォータマークコードワードを生成する。後述するように、複数の部分を有するコードワードを生成することにより、ウォータマークを階層的に構築することもできる。ここでは、例示的に20ビットのコードワードについて説明する。20ビットのコードワードは、可能なデータ値として、一千万以上 (1048576個) のコードワードを提供する。

【0055】

ここで説明する具体例では、20ビットのコードワードをそれぞれ10ビットからなる2つの部分に分割する。これを図9に示す。第1の10ビットは、ウォータマークの第1の部分 WM_1 を生成するために使用される。第2の10ビットは、ウォータマークの第2の部分 WM_2 を生成するために使用される。第1の部分 WM_1 及び第2の部分 WM_2 は、上述したように、ウォータマークを付すべき画像に埋め込まれる。

【0056】

好適な具体例においては、第1の部分 WM_1 は、コードワード生成器8の一部を構成する疑似乱数生成器によって生成された第1のコードワード係数からなる1つのコードワードを生成することにより形成される。これらの数値は、図9に示すように、基礎シード値 s

eedから生成される。基礎シード値は、ソース画像のサンプルから生成してもよい。

【0057】

ウォータマークの10ビットの第1の部分WM1では、1024個の可能な各データ値は、基礎シード値から生成されたコードワードの第1の部分WM1をシフトすることにより得られる1024個の可能なシフトによって表される。図9に示すように、このシフトは、0から1023の可能な値を有する。

【0058】

ウォータマークの第2の部分WM2は、ウォータマークの第1の部分WM1とは独立して生成される。第1の部分WM1に適用されたシフトは、1024個の可能な補助的シード値(supplementary seeds)の1つにマッピングされる。すなわち、コードワードのi番目のシフト $X1 \rightarrow i = X1i$ は、固有の補助的シード値(seedi)を特定する。この補助的シード値から、図9においてX2として示されている更なるコードワードが生成される。このように、第1の部分WM1を構成する第1のコードワード $X1i$ のシフトと、第2の部分WM2用の第2のコードワード $X2i$ を生成するために使用されるシード値との間には、所定の固有の関係がある。ここで、更なる1024個の可能な値を表すために、ウォータマークの第2の部分WM2は、第2の部分WM2の10ビット値に基づいてシフトされる。図10に示すように、この処理により値の階層構造が形成される。第1の部分WM1によって生成される第1の1024ビットは、第2の部分WM2を構成するコードワードの指標を提供する。第2の部分WM2から生成されるコードワードの可能なシフトは、階層構造の第2レベルにおける第2の1024ビットの値の組を提供する。

【0059】

本発明の具体例では、複数の階層に基づいてウォータマークが付された画像を特定することができる。例えば、第1の部分WM1は、画像が配信された国、地域、又は地域の一部分を特定するために使用することができる。一方、階層の第2レベルは、地域の第2の部分、例えばウォータマークが付された画像が再生された町や映画館を特定するために使用することができる。これにより、ウォータマークが付された画像が再生され、この画像からオフエンディングコピーが作成された場所をより速く、より正確に特定することができる。

【0060】

2つの部分WM1、WM2を有するコードワードを生成する更なる利点は、図6に示すフーリエ変換相関器を用いて、2つの階層レベルのそれぞれに1024個の値のうちのどの値が存在するかを効率的に特定できる点にある。この組合せでは、ウォータマークの第2の部分WM2は、第2のコードワードの1024個の可能なシフトから生成されているため、更なるフーリエ変換復号を用いて、コードワードの第2の部分WM2の可能なシフトを特定することができる。

【0061】

2つの関連する部分を有するウォータマークコードワードを生成することにより、コルジョンアタックが成功する確率を低減することができる。上述のように、これらのコードワードの部分のいずれか一方又は両方の順序を変更した後に画像に埋め込んでもよい。

【0062】

他の適用例

ウォータマークシステムの符号化データ処理装置は、上述した映写機及びウェブサーバに加えて、他の用途にも適用することができる。例えば、本発明は、通信装置から信号を受信し、この受信した信号にコードワードを導入することにより情報にウォータマークを付す受信機／デコーダにも適用することができる。例えば、セットトップボックスは、放送の「ヘッドエンド」機器又はマルチキャスト機器からテレビジョン及びビデオ信号を受信する。このような適用例では、符号化データ処理装置は、セットトップボックスの一部を構成し、信号を受信及びデコードする際にビデオ信号にウォータマークコードワードを導入する。一具体例においては、このウォータマークコードワードは、ビデオ信号を受信及

びデコードしたセットトップボックスを固有に特定する。

【0063】

更に、本発明は、衛星からデジタル映画データ (digital cinema film) を受信するデジタル映画受信機にも適用することができる。このデジタル映画受信機は、デジタル映画を表す信号を受信し、この信号をデコードしてデジタル映画を再生する。この受信機は、デコードされた映画信号にウォーターマークコードワードを導入する符号化データ処理装置を備える。ウォーターマークコードワードは、例えば、デジタル映画データを受信したデジタル映画受信機を固有に特定する。

【0064】

更に、本発明は、メモリ及びメモリコントローラを備えるデジタルカメラ又はカムコーダ等にも適用することができる。この適用例では、本発明に係る符号化データ処理装置は、メモリに記憶されているウォーターマークコードワードをデジタルカメラ等によって撮影されたビデオ信号に導入する。この適用例においては、コードワードは予めメモリに記憶されており、したがって、符号化データ処理装置は、コードワード生成器を備えていない。メモリに記憶されているコードワードは、メモリコントローラの制御の下、ビデオ信号に埋め込まれ、これによりビデオ信号を固有に又は疑似固有的 (quasi-unique ly) に特定する。

【0065】

更なる具体例においては、本発明に基づく符号化データ処理装置は、連続的な画像又は動画を構成する複数の異なるデジタル画像のフレームのそれぞれに一連のウォーターマークコードワードを個別に埋め込む。これらのコードワードは、互いに関連性を有していてもよく、これらのコードワードにより、各フレームに対応する画像を個別に識別することができるようになる。

【0066】

本発明の更なる様々な側面及び特徴は、添付の請求の範囲において定義されている。この請求の範囲から逸脱することなく、上述した実施の形態を様々に変更することができる。

【図面の簡単な説明】

【図1】符号化画像処理装置の構成を示すブロック図である。

【図2】検出画像処理装置の構成を示すブロック図である。

【図3】図3Aはオリジナル画像を示し、図3Bはウォーターマークが付された画像を示し、図3Cは登録された画像を示す図である。

【図4】N個のコードワードの組の各コードワードに関する相関結果の具体例を示すグラフ図である。

【図5】図5Aはオリジナル画像Iのサンプルに対応するグラフ図であり、図5Bはウォーターマークが付された画像W'に対応するグラフ図であり、図5Cはオリジナル画像とウォーターマークが付された画像との離散サンプルシフト毎の相関結果を示すグラフ図である。

【図6】図2に示す検出データプロセッサの一部である相関器の構成を示すブロック図である。

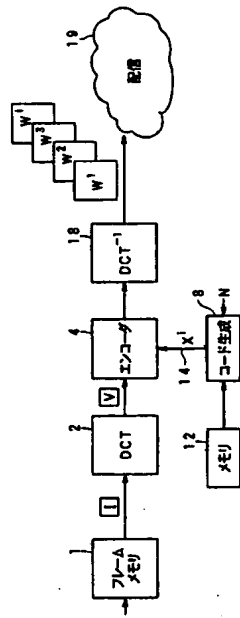
【図7】符号化画像データ処理装置によってウォーターマークが付された画像を作成する手順を示すフローチャートである。

【図8】図2に示す検出データプロセッサによって、受信したウォーターマークが付された画像からウォーターマークを特定する処理を示すフローチャートである。

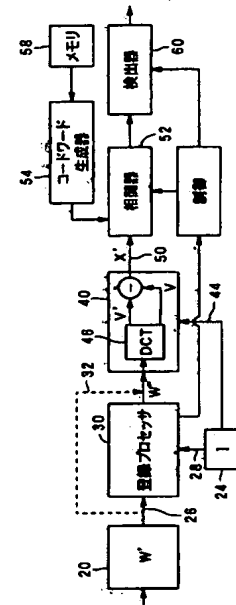
【図9】少なくとも2つの部分を有するコードワード係数を生成する処理を説明する図である。

【図10】図9に示す処理により生成された2つの部分を有するコードワードを用いて構築される階層的情報を示す図である。

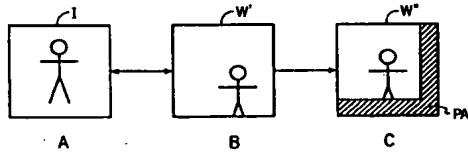
【図 1】



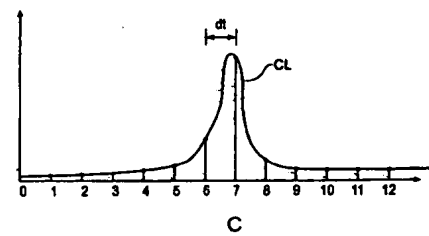
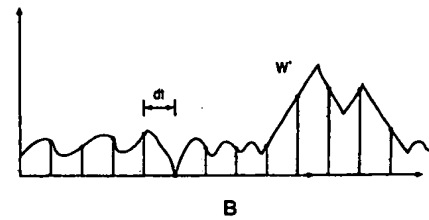
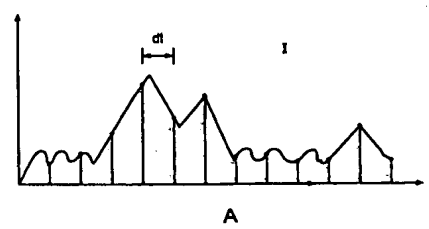
【図 2】



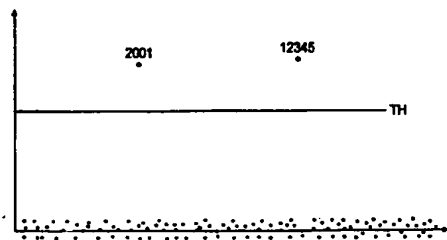
【図 3】



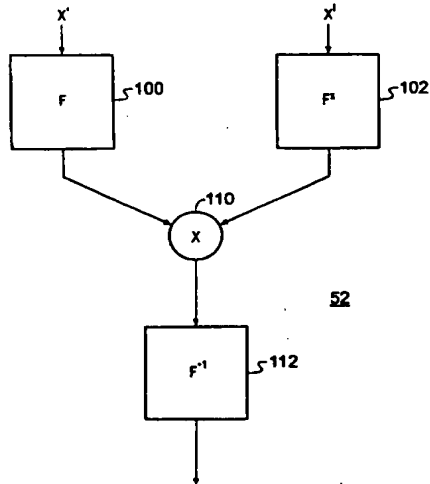
【図 5】



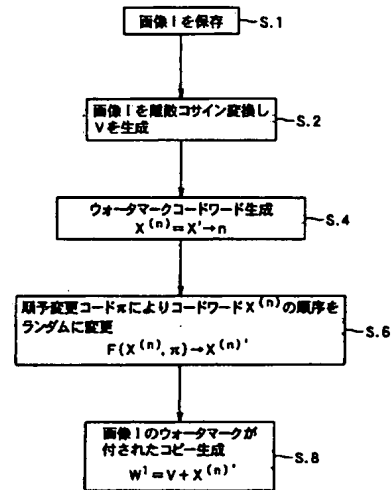
【図 4】



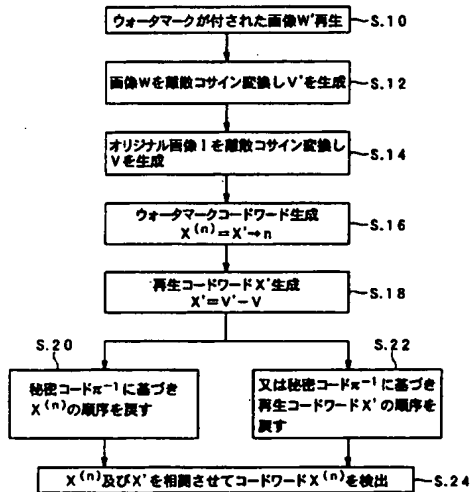
【図 6】



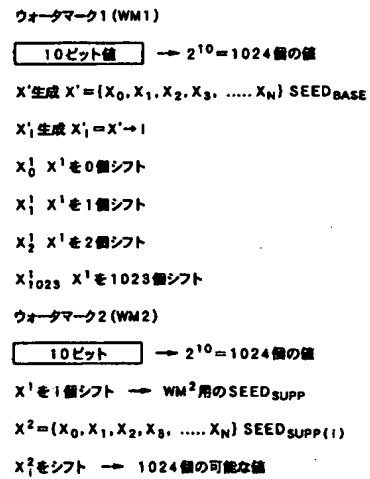
【図 7】



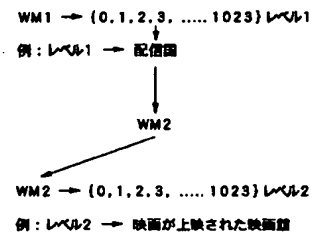
【図 8】



【図 9】



【図 10】



フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 L 9/36

H 0 4 L 9/00 6 8 5

H 0 4 N 7/08

H 0 4 N 7/08 Z

H 0 4 N 7/081

H 0 4 N 7/133 Z

H 0 4 N 7/30

G 1 0 L 9/00 E

(72)発明者 ベリー ジェイソン チャールズ

イギリス国 K T 1 3 0 X W サリー ウェイブリッジ ブルックランズ ザ ハイツ (番地なし) ソニー ユナイテッド キングダム リミテッド内

(72)発明者 タブソン ダニエル ワレン

イギリス国 K T 1 3 0 X W サリー ウェイブリッジ ブルックランズ ザ ハイツ (番地なし) ソニー ユナイテッド キングダム リミテッド内

Fターム(参考) 5B057 CB19 CE08 CH01 CH11

5C059 KK43 MA23 PP01 RC35 SS08 SS11 UA02 UA05

5C063 AC01 CA23 DA07 DA13 DB09

5C076 AA14 BA06

5J104 AA13 NA13 NA15 NA23

【外国語明細書】

1 Title of Invention

DATA PROCESSING APPARATUS AND METHOD

2 Claims

1. An encoding data processing apparatus for generating at least one marked copy of an original item of material by introducing one of a predetermined set of code words into a copy of said material item, said apparatus comprising,

a code word generator operable to provide said code word having a plurality of code word coefficients, and

an encoding processor operable to combine the code word coefficients with said material, wherein

each of said plurality of code words of said set is uniquely associated with a data word having first and second fields, each of a set of values of said first field being represented as a first part of said code word having a first plurality of coefficients, and said second field is represented as a second part of said code word having a second plurality of coefficients.

2. An encoding data processing apparatus as claimed in Claim 1, wherein each value of said first field is represented as a predetermined cyclic shift of said first plurality of code word coefficients of said first part of said code word.

3. An encoding data processing apparatus as claimed in Claim 2, wherein said code word generator includes a pseudo-random number generator operable to generate pseudo-random numbers from which said first part of said code word is derived, said value of the first field defining a predetermined cyclic shift of said first code word coefficients.

4. An encoding data processing apparatus as claimed in Claims 1, 2 or 3, wherein said second plurality of coefficients of said second part of said code word are derived from pseudo-random numbers generated using one of a plurality of supplementary seeds identified by said value of said first field, each of the values of said second data field being represented as a corresponding shift of said second plurality of coefficients.

5. An encoding data processing apparatus as claimed in any preceding Claim, wherein said code word generator is operable to generate a first seed value for generating said first plurality of code word coefficients from samples of said material item.

6. An encoding processor as claimed in any preceding Claim, wherein said encoding processor is operable to permute at least one of said first plurality of code word coefficients and said second plurality of code word coefficients in accordance with a permutation code.

7. An encoding data processing apparatus as claimed in any preceding Claim, comprising

a discrete cosine transform processor operable to transform said material item into the discrete cosine transform domain, said material item in said discrete cosine transform domain being represented as a plurality of discrete cosine transform coefficients, wherein said encoding processor is operable to combine said code word with said material item by adding each of said first and second code word coefficients to a corresponding one of said discrete cosine transform coefficients, and

an inverse discrete cosine transform processor operable to form said marked copy of said material item by performing an inverse discrete cosine transform on said discrete cosine transformed image to which said code word has been added by said encoding processor.

8. A cinema projector including an encoding data processing apparatus according to any of Claims 1 to 7, wherein said data processing apparatus is operable to receive at least one of audio signals and image signals before reproduction, and to introduce a code word into said at least one of audio signals and image signals before reproduction.

9. A web server operable to provide material items for downloading via the Internet, said web server including an encoding data processing apparatus according to any of Claims 1 to 7, wherein said data processing apparatus is operable

to receive material items and to introduce a code word into said material items before said material items are downloaded.

10. A detecting data processing apparatus operable to identify at least one of set of code words present in a marked version of a material item, said marked version having been formed by combining each of a plurality of samples of an original version of said material item with one of a corresponding plurality of code word coefficients, each code word being uniquely associated with a data word having first and second fields, each of a set of values of said first field being represented as a first part of said code word having a first plurality of coefficients, and said second field being represented as a second part of said code word having a second plurality of coefficients, and each value of said first field being represented as a predetermined cyclic shift of said first plurality of code word coefficients of said first part of said code word, said detecting data processing apparatus comprising

- a decoding processor operable to generate a recovered code word from said marked material item, and

- a detection processor operable to detect at least one first data field value and at least one second data field value by

- correlating the first part of the recovered code word with a first part of each regenerated code word from the set of code words to generate a correlation value for each regenerated code word,

- detecting the value of the first field value from a corresponding correlation value exceeding a predetermined threshold,

- correlating the second part of the recovered code word with a second part of each regenerated code word from the set of code words to generate a second correlation value for each regenerated code word, and

- detecting the value of the second field value from a corresponding second correlation value exceeding a predetermined threshold.

11. A detecting data processing apparatus as claimed in Claim 10, wherein said detection processor is operable to form said correlation value for said first part of said recovered code word and the first part of each of said regenerated code words by

forming a Fourier transform of a part corresponding to the first part of said recovered code word,

forming a Fourier transform of said first plurality of code word coefficients of the first part of the regenerated code word,

forming the complex conjugate of one of the Fourier transform of the first part of the recovered code word and the Fourier transform of the first part of the regenerated code word,

forming intermediate product samples by multiplying each of said Fourier transform samples of said first part of said recovered code word and the corresponding Fourier transform samples of said first part of said regenerated code word, and

forming correlation samples for the first part of the recovered code word by forming an inverse transform of said intermediate product samples, each of said correlation value samples providing the correlation value for the first part of said code words.

12. A detecting data processing apparatus as claimed in Claim 10 or 11, wherein said second plurality of coefficients of said second part of said code word are derived from pseudo-random numbers generated from one of a plurality of supplementary seeds identified by said value of said first field, each of the values of said second data field being represented as a corresponding shift of said second plurality of coefficients, wherein

said decoding processor is operable to identify a supplementary seed from the set of supplementary seeds, indicated from said first field value detected from said correlation values, and

said detection processor is operable to regenerate said second plurality of code word coefficients from said identified supplementary seed and to identify the value of said second data field from a shift of said second code word coefficients with respect to said second part of said recovered code word.

13. A detecting data processing apparatus as claimed in Claim 12, wherein said detection processor is operable to identify the value of the shift of said regenerated second plurality of coefficients with respect to said second part of said

recovered code word by correlating said regenerated second plurality of coefficients with said second part of said recovered code word.

14. A detecting data processing apparatus as claimed in Claim 13, wherein said detection processor is operable to correlate said regenerated second plurality of coefficients with said second part of said recovered code word by

forming a Fourier transform of the second part of said recovered code word,

forming a Fourier transform of said second plurality of code word coefficients of the second part of the regenerated code word,

forming the complex conjugate of one of the Fourier transform of the second part of the recovered code word and the Fourier transform of the second part of regenerated code word,

forming intermediate product samples by multiplying each of said Fourier transform samples of said second part of said recovered code word and the corresponding Fourier transform samples of said regenerated second code word part,

forming correlation samples for the second part of the recovered code word by forming an inverse transform of said intermediate product samples, each of said correlation value samples providing the correlation value for the second part of said code words.

15. A detecting data processor as claimed in any of Claims 10 to 14, wherein at least one of said first plurality of code word coefficients and said second plurality of code word coefficients forming said first and second parts of said code word are combined with the material in accordance with a permutation code, wherein said decoding processor is operable to reverse the permutation of at least one of said first and said second recovered code word coefficients in accordance with said permutation code.

16. A detecting data processor as claimed in any of Claims 10 to 14, wherein at least one of said first plurality of code word coefficients and said second plurality of code word coefficients forming said first and second parts of said code word are combined with the material in accordance with a permutation code, wherein

one of said detecting processor is operable to reverse the permutation of at least one of said first and said second re-generated code word coefficients in accordance with said permutation code.

17. A system for identifying the recipient of a material item, said system comprising

an encoding data processor according to any of Claims 1 to 7, operable to generate said marked material item by introducing a code word generated from a seed uniquely identifying said recipient, and

a detecting data processor according to any of Claims 10 to 16, operable to detect with a predetermined false positive probability the recipient by detecting the presence of the code word in said material.

18. A method of generating at least one marked version of an original item of material by introducing one of a predetermined set of code words into a copy of said original material item, said method comprising,

forming said code word by generating a plurality of code word coefficients, and

combining the code word coefficients with said material, wherein

each of said plurality of code words of said set is uniquely associated with a data word having first and second fields, each of a set of values of said first field being represented as a first part of said code word having a first plurality of coefficients, and said second field is represented as a second part of said code word having a second plurality of coefficients.

19. A method of identifying at least one of set of code words present in a marked version of a material item, said marked version having been formed by combining each of a plurality of samples of an original version of said material item with one of a corresponding plurality of code word coefficients, each code word being uniquely associated with a data word having first and second fields, each of a set of values of said first field being represented as a first part of said code word having a first plurality of coefficients, and said second field being represented as a second part

of said code word having a second plurality of coefficients, and each value of said first field being represented as a predetermined cyclic shift of said first plurality of code word coefficients of said first part of said code word, said method comprising

generating a recovered code word from said marked material item, and

detecting at least one first data field value and at least one second data field value by

correlating the first part of the recovered code word with a first part of each regenerated code word from the set of code words to generate a correlation value for each regenerated code word,

detecting the value of the first field value from a corresponding correlation value exceeding a predetermined threshold,

correlating the second part of the recovered code word with a second part of each regenerated code word from the set of code words to generate a second correlation value for each regenerated code word, and

detecting the value of the second field value from a corresponding second correlation value exceeding a predetermined threshold.

20. A data signal representing a material item to which a code word has been added by the data processing apparatus according to any of Claims 1 to 7.

21. A data carrier having recorded thereon a data signal according to Claim 20.

22. A computer program providing computer executable instructions, which when loaded onto a data processor configures the data processor to operate as the encoding data processing apparatus according to any of Claims 1 to 7 or the detecting data processor according to any of Claims 10 to 16.

23. A computer program providing computer executable instructions, which when loaded on to a data processor causes the data processor to perform the method according to Claim 18 or 19.

24. A computer program product having a computer readable medium having recorded thereon information signals representative of the computer program claimed in any of Claims 22 or 23.

25. A receiver operable to receive signals representative of material items, comprising

an encoding data processing apparatus according to any of Claims 1 to 7, operable to combine at least one code word with the received signals, said code word being provided to identify uniquely said received signals.

26. A detecting or an encoding data processing apparatus as herein before described with reference to the accompanying drawings.

27. A method of identifying at least one of a predetermined set of code words or a method of generating at least one marked copy of an original item of material as herein before described with reference to the accompanying drawings.

3 Detailed Description of Invention

Field of Invention

The present invention relates to encoding data processing apparatus and methods, which are arranged to embed code words into versions of material items. In some applications the code words are used to uniquely identify the material items.

Correspondingly, the present invention also relates to data processing apparatus and methods operable to detect one or more code words, which may be present in a material item.

Background of the Invention

A process in which information is embedded in material for the purpose of identifying the material is referred to as watermarking.

Identification code words are applied to versions of material items for the purpose of identifying the version of the material item. Watermarking can provide, therefore, a facility for identifying a recipient of a particular version of the material. As such, if the material is copied or used in a way, which is inconsistent with the wishes of the distributor of the material, the distributor can identify the material version from the identification code word and take appropriate action.

In this description, an item of material, which is copied or used in a way, which is inconsistent with the wishes of the originator, owner, creator or distributor of the material, will be referred to for convenience as an offending item of material or offending material.

The material could be any of video, audio, audio/video material, software programs, digital documents or any type of information bearing material.

For a watermarking scheme to be successful, it should be as difficult as possible for the users to collude in order to mask or remove the identification code words. It should also be as difficult as possible for users to collude to alter the identification code word to the effect that one of the other users is falsely indicated as the perpetrator of an offending item of material. Such an attempt by users to collude to either mask the code word or alter the code word to indicate another user is known as a collusion attack.

Any watermarking scheme should be arranged to make it difficult for users receiving copies of the same material to launch a successful collusion attack. A watermarking scheme should therefore with high probability identify a marked material item, which has been the subject of a collusion attack. This is achieved by identifying a code word recovered from the offending material. Conversely, there should be a low probability of not detecting a code word when a code word is present (false negative probability). In addition the probability of falsely detecting a user as guilty of taking part in a collusion attack, when this user has not taken part, should be as low as possible (false positive probability).

US Patent Serial No. 5, 664, 018 discloses a watermarking process in which a plurality of copies of material items are marked with a digital watermark formed from a code word having a predetermined number of coefficients. The watermarked material item is for example an image. The apparatus for introducing the watermark transforms the image into the Discrete Cosine Transform (DCT) domain. The digital watermark is formed from a set of randomly distributed coefficients having a normal distribution. In the DCT domain each code word coefficient is added to a corresponding one of the DCT coefficients. The watermarked image is formed by performing an inverse DCT. A related publication entitled "Resistance of Digital Watermarks to Collusion Attacks", by J. Kilian, F. T. Leighton et al, published by MIT, July 27, 1998, provides a detailed mathematical analysis of this watermarking process to prove its resistance to attack.

Summary of the Invention

According to an aspect of the present invention there is provided an encoding data processing apparatus for generating at least one marked copy of an original item of material by introducing one of a predetermined set of code words into a copy of the material item. The apparatus comprises a code word generator operable to provide the code word having a plurality of code word coefficients, and an encoding processor operable to combine the code word coefficients with the material. Each of the plurality of code words of the set is uniquely associated with a data word having first and second fields. Each of a set of values of the first field is represented as a first part

of the code word having a first plurality of coefficients, and the second field is represented as a second part of the code word having a second plurality of coefficients.

The present invention provides a facility for generating watermark code words having a hierarchy of values. By providing watermark code words with first and second parts, a data word with first and second fields can be uniquely identified. The first and second fields can be assigned to different associated parameters such as for example address parameters. The first field could therefore identify the country of distribution of the material, whereas the second field could identify a particular distribution outlet within the country.

In preferred embodiments each value of the first field is represented as a predetermined cyclic shift of the first plurality of code word coefficients forming the first part of the code word. In order to implement a practically useful system the number of uniquely identifiable code words in the set should be as high as possible. For a consumer distributed product such as a video or a film for display at a cinema, there should be in the order of a million or preferably tens of millions of code words in the set. As such, it will be appreciated that correlating each of the regenerated code words and the recovered code word to identify the recovered code word and therefore the first and second fields, represents a considerable computational task. Embodiments of the present invention are provided with an advantage with respect to calculating the correlation values for at least the first part of the code words in the set. This is provided by forming at least the first part of the code words of the set by generating a first plurality of code word coefficients and generating other code words by cyclically shifting the first plurality of code word coefficients. As such, the correlation values for all first parts of the code words of the set can be calculated using a Fourier transform correlator. As will be explained, the Fourier transform correlator provides the correlation values for the set in one operation, substantially reducing the computational task.

The second plurality of coefficients of the second part of the code word may be derived from pseudo-random numbers generated by a pseudo-random number generator using one of a plurality of supplementary seeds. The supplementary seed for generating the second part of the code word may be identified by the value of the first field or correspondingly the relative shift of the first plurality of coefficients. Each of

the values of the second data field is represented as a corresponding shift of the second plurality of coefficients. By forming the watermark from first and second parts, a hierarchy of data words can be defined. Furthermore, the code words, which are defined by each data word, are provided with improved robustness to a collusion attack and can be efficiently detected using a Fourier transform correlator.

In preferred embodiments, the encoding processor is operable to permute the order in which at least one of the first and second code word coefficients are combined with the material in accordance with a permutation code. Correspondingly, in preferred embodiments the detecting data processor is arranged to reverse the permutation of either the re-generated first and/or second code word coefficients or the recovered first and/or second code word coefficients in order to perform the correlation values. Permuting the code word coefficients provides an advantage of reducing the likelihood of a successful collusion attack, which may increase by forming the code words from cyclically shifting the first code word.

According to an aspect of the present invention there is provided a detecting data processing apparatus as defined in the appended claims. As will be explained, example embodiments of the invention are arranged to identify the first and second field values from the first and second parts of the watermark. Advantageously, this is achieved by forming a correlation of the first plurality of coefficients from a recovered version of the code word with respect to the first part of each of the code words of the set. This correlation is achieved using a Fourier transform correlator. The first field value is determined by a correlation value produced by the Fourier transform correlator which indicates the shift of the first plurality of code word coefficients. The first field then identifies a supplementary seed from which the second plurality of code word coefficients, forming the second part of the watermark, were generated. By again using a Fourier transform correlator, the value of the second field can be identified from correlation values indicating the shift of the second plurality of code word coefficients.

Various further aspects and features of the present invention are defined in the appended claims.

Description of Preferred Embodiments

Watermarking System Overview

An example embodiment of the present invention will now be described with reference to protecting video images. The number of users to which the video images are to be distributed determines the number of copies. To each copy an identification code word is added which identifies the copy assigned to one of the users.

Video images are one example of material, which can be protected by embedding a digital code word. Other examples of material, which can be protected by embedding a code word, include software programs, digital documents, music, audio signals and any other information-bearing signal.

An example of an encoding image processing apparatus, which is arranged to introduce an identification code word into a copy of an original image, is shown in Figure 1. An original image I is received from a source and stored in a frame store 1. This original image is to be reproduced as a plurality of water marked copies, each of which is marked with a uniquely identifiable code word. The original image is passed to a Discrete Cosine Transform (DCT) processor 2, which divides the image into 8×8 pixel blocks and forms a DCT of each of the 8×8 pixel blocks. The DCT processor 2 therefore forms a DCT transformed image V .

In the following description the term "samples" will be used to refer to discrete samples from which an image (or indeed any other type of material) is comprised. The samples may be luminance samples of the image, which is otherwise, produce from the image pixels. Therefore, where appropriate the terms samples and pixels are interchangeable.

The DCT image V is fed to an encoding processor 4. The encoding processor 4 also receives identification code words from an identification code word generator 8.

The code word generator 8 is provided with a plurality of seeds, each seed being used to generate one of the corresponding code words. Each of the generated code words may be embedded in a copy of the original image to form a watermarked image. The code word generator 8 is provided with a pseudo random number generator. The pseudo random number generator produces the code word coefficients to form a particular code word. In preferred embodiments the coefficients of the code

words are generated in accordance with a normal distribution. However, the coefficients of the code word are otherwise predetermined in accordance with the seed, which is used to initialise the random number generator. Thus for each code word there is a corresponding seed which is store in a data store 12. Therefore it will be understood that to generate the code word X^i , $seed_i$ is retrieved from memory 12 and used to initialise the random number generator within the code word generator 8.

In the following description the DCT version of the original image is represented as V , where;

$$V = \{v_i\} = \{v_1, v_2, v_3, v_4, \dots, v_N\}$$

and v_i are the DCT coefficients of the image. In other embodiments the samples of the image v_i could represent samples of the image in the spatial domain or in an alternative domain.

Each of the code words X^i comprises a plurality of n code word coefficients, where;

$$X^i = \{x'_j\} = \{x'_1, x'_2, x'_3, x'_4, \dots, x'_n\}$$

The number of code word coefficients n corresponds to the number or samples of the original image V . However, a different number of coefficients is possible, and will be set in dependence upon a particular application.

A vector of code word coefficients X^i forming the i -th code word is then passed via channel 14 to the encoder 4. The encoder 4 is arranged to form a watermarked image W^i by adding the code word X^i to the image V . Effectively, therefore, as represented in the equation below, each of the code word coefficients is added to a different one of the coefficients of the image to form the watermark image W^i .

$$W^i = V + X^i$$

$$W^i = v_1 + x'_1, v_2 + x'_2, v_3 + x'_3, v_4 + x'_4, \dots, v_n + x'_n$$

As shown in Figure 1, the watermarked images W^i are formed at the output of the image processing apparatus by an forming inverse DCT of the image produced at the output of the encoding processor 4 by the inverse DCT processor 18.

Therefore as represented in Figure 1 at the output of the encoder 4 a set of the watermarked images can be produced. For a data word of up to 20-bits, one of 10 000

000 code words can be selected to generate 10 million watermarked W^i versions of the original image I .

Although the code word provides the facility for uniquely identifying a marked copy W^i of the image I , in other embodiments the 20 bits can provide a facility for communicating data within the image. As will be appreciated therefore, the 20 bits used to select the identification code word can provide a 20 bit pay-load for communicating data within the image V .

The encoding image processing apparatus which is arranged to produce the watermarked images shown in Figure 1 may be incorporated into a variety of products for different scenarios in which embodiments of the present invention find application. For example, the encoding image processing apparatus may be connected to a web site or web server from which the watermarked images may be downloaded. Before downloading a copy of the image, a unique code word is introduced into the downloaded image, which can be used to detect the recipient of the downloaded image at some later point in time.

In another application the encoding image processor forms part of a digital cinema projector in which the identification code word is added during projection of the image at, for example, a cinema. Thus, the code word is arranged to identify the projector and the cinema at which the images are being reproduced. Accordingly, the identification code word can be identified within a pirate copy produced from the images projected by the cinema projector in order to identify the projector and the cinema from which pirate copies were produced. Correspondingly, a watermarked image may be reproduced as a photograph or printout in which a reproduction or copy may be made and distributed. Generally therefore, the distribution of the watermarked images produced by the encoding image processing apparatus shown in Figure 1 is represented by a distribution cloud 19.

Detecting Processor

A detecting image processing apparatus which is arranged to detect one or more of the code words, which may be present in an offending marked image is shown in Figure 2. Generally, the image processor shown in Figure 2 operates to identify one or more of the code words, which may be present in an offending copy of the image.

The offending version of the watermarked image W' is received from a source and stored in a frame store 20. Also stored in the frame store 24 is the original version of the image I , since the detection process performed by the image processor requires the original version of the image. The offending watermarked image W' and the original version of the image are then fed via connecting channels 26, 28 to a registration processor 30.

As already explained, the offending version of the image W' may have been produced by photographing or otherwise reproducing a part of the watermarked image W^i . As such, in order to improve the likelihood of detecting the identification code word, the registration processor 30 is arranged to substantially align the offending image with the original version of the image present in the data stores 20 and 24. The purpose of this alignment is to provide a correspondence between the original image samples I and the corresponding samples of the watermarked image W^i to which the code word coefficients have been added.

The effects of the registration are illustrated in Figure 3. In Figure 3 an example of the original image I is shown with respect to an offending marked version of the image W' . As illustrated in Figure 3, the watermarked image W' is offset with respect to the original image I and this may be due to the relative aspect view of the camera from which the offending version of the watermarked image was produced.

In order to recover a representation of the code word coefficients, the correct samples of the original image should be subtracted from the corresponding samples of the marked offending image. To this end, the two images are aligned. As shown in Figure 3, the registered image W'' has a peripheral area PA which includes parts which were not present in the original image.

As will be appreciated in other embodiments, the registration processor 30 may not be used because the offending image W' may be already substantially aligned to the original version of the image I , such as, for example, if the offending version was downloaded via the Internet. Accordingly, the detecting image processor is provided with an alternative channel 32, which communicates the marked image directly to the recovery processor 40.

The registered image W'' is received by a recovery processor 40. The recovery processor 40 also receives a copy of the original image I via a second channel 44. The registered image W'' and the original image I are transformed by a DCT transform processor 46 into the DCT domain. An estimated code word X' is then formed by subtracting the samples of the DCT domain marked image V' from the DCT domain samples of the original image V as expressed by the following equations:

$$\begin{aligned} X' &= V' - V \\ &= v'_1 - v_1, v'_2 - v_2, v'_3 - v_3, v'_4 - v_4, \dots, v'_n - v_n, \\ &= x'_1, x'_2, x'_3, x'_4, \dots, x'_n \end{aligned}$$

The output of the recovery processor 40 therefore provides on a connecting channel 50 an estimate of the coefficients of the code word which is to be identified. The recovered code word X' is then fed to a first input of a correlator 52. The correlator 52 also receives on a second input the regenerated code words X^i produced by the code word generator 54. The code word generator 54 operates in the same way as the code word generator 8 which produces all possible code words of the set, using the predetermined seeds which identify uniquely the code words from a store 58.

The correlator 52 forms n similarity $sim(i)$ values. In one embodiment, the similarity value is produced by forming a correlation in accordance with following equation:

$$sim(i) = \frac{X' \cdot X^i}{\sqrt{X' \cdot X'}} = \frac{x'_1 \cdot x^i_1 + x'_2 \cdot x^i_2 + x'_3 \cdot x^i_3 + \dots + x'_n \cdot x^i_n}{\sqrt{x'_1 \cdot x^i_1 + x'_2 \cdot x^i_2 + x'_3 \cdot x^i_3 + \dots + x'_n \cdot x^i_n}}$$

Each of the n similarity values $sim(i)$ is then fed to a detector 60. The detector 60 then analyses the similarity values $sim(i)$ produced for each of the n possible code words. As an example, the similarity values produced by the correlator 52 are shown in Figure 4 with respect to a threshold TH for each of the possible code words. As shown in Figure 4, two code words are above the threshold, 2001, 12345. As such, the detecting processor concludes that the watermarked version associated with code word 2001 and code word 12345 must have colluded in order to form the offending image. Therefore, in accordance with a false positive detection probability, determined from the population size, which in this case is 10 million and the watermarking strength α ,

the height of the threshold TH can be set in order to guarantee the false detection probability. As in the example in Figure 4, if the similarity values produced by the correlator 52 exceed the threshold then, with this false positive probability, the recipients of the marked image are considered to have colluded to form the offending watermarked version of the image W^i .

The following sections illustrate advantages and features of the operation of the watermarking system illustrated in Figures 1 and 2.

Registration

The process of aligning the offending marked version of the image with the copy of the original image comprises correlating the samples of the original image with respect to the marked image. The correlation is performed for different shifts of the respective samples of the images. This is illustrated in Figure 5.

Figure 5A provides an illustration of discrete samples of the original image I , whereas Figure 5B provides an illustration of discrete samples of the offending watermarked image W^i . As illustrated in the Figures 5A and 5B, the sampling rate provides a temporal difference between samples of dt . A result of shifting each of the sets of samples from the images and correlating the discrete samples is illustrated in Figure 5C.

As shown in Figure 5C, for a shift of between 6 and 7 samples, the correlation peak is highest. The offending watermarked image is therefore shifted by this amount with respect to the original image to perform registration.

Fourier Decoding

As explained, with reference to Figures 1 and 2, the watermarking system can provide a facility for generating 10 million watermarked versions of an original image. This is effected using a 20-bit watermark value. However, as explained, in order to detect the presence of one of the code words in an offending watermarked image, the detecting image processor must correlate each of the possible code words in the set of 10 million code words with respect to a recovered code word from the image. As will be appreciated, this represents a considerable computational task.

A correlator embodying the present invention provides a significant advantage in reducing the computational effort and therefore the time taken to detect the presence of a code word in an offending watermarked image. A correlator in accordance with the embodiment of the present invention is illustrated in Figure 6. The correlator shown in Figure 6 takes advantage of an alternative technique for calculating the correlation sum shown above. In accordance with this technique the correlation sum is calculated in accordance with the following equation:

$F^{-1}[F(X')F(X^{(1)})^*]$, where $F(A)$ is the Fourier transform of A and $F^{-1}(A)$ is the inverse Fourier transform of A.

The correlator 52 shown in Figure 7 therefore comprises a first Fourier transform processor 100, and a second Fourier transform processor 102. Fourier transform processors 100, 102 may be implemented using Fast Fourier transform algorithms. The second Fourier transform processor 102 also forms the complex conjugate of the Fourier transform of the regenerated code word X^j . The Fourier transform of the recovered code word X' and the complex conjugate of the Fourier transform of the regenerated code word X^j are fed to first and second inputs of a multiplier 110. The multiplier 110 multiplies the respective samples from each of the Fourier transform processors 100, 102 and feeds the multiplied samples to an inverse Fourier transform processor 112. At the output of the correlator an inverse Fourier transform of the multiplied signals samples is formed.

As will be appreciated, the implementation of the correlator 52 shown in Figure 6 provides an advantage in terms of time taken to compute the correlation for the n sample values of the regenerated code word X^j and the recovered code word X' . This is because the Fourier processors 100, 102, 112 can be formed from FFT integrated circuits such as, for example, are available as ASICs. Furthermore, the inverse Fourier transform provided at the output of the correlator 52 provides n similarity values $sim(i)$ corresponding to n correlation sums. However, in order to utilise the properties of the correlator 52, shown in Figure 6 the code words are arranged to be generated by cyclically shifting one code word generated $X^{(j)}$ using a particular seed for the random number generator. This is illustrated below. As shown below, the first code word $X^{(1)}$ is represented as values x_1 to x_n which corresponds to the pseudo randomly produced

numbers from the code word generator 8. However, the second code word $X^{(2)}$ is produced by performing a cyclic shift on the first code word $X^{(1)}$. Correspondingly, each of the other code words are produced by correspondingly cyclically shifting further the code word $X^{(1)}$ until the n -th code word is a code word shifted by $n-1$ positions.

$$X^{(1)} \rightarrow (x_1, x_2, x_3, x_4, \dots, x_{n-1}, x_n)$$

$$X^{(2)} \rightarrow (x_2, x_3, x_4, \dots, x_{n-1}, x_n, x_1)$$

$$X^{(3)} \rightarrow (x_3, x_4, \dots, x_{n-1}, x_n, x_1, x_2)$$

$$\dots \dots \dots \dots \dots \dots \dots$$

$$X^{(n)} \rightarrow (x_n, x_1, x_2, x_3, x_4, \dots, x_{n-2}, x_{n-1})$$

By using this set of code words to form part of, or the whole of, the set of code words produced by the encoding image processor, the Fourier transform correlator 52 can be used to generate in one operation all similarity values for all of the n code words. Therefore, as illustrated above, the corresponding shift of 1 to n of the original code word provides the n similarity values $sim(i)$, and as illustrated in Figure 4, for at least one of the code words, a large similarity value $sim(i)$ is produced. Therefore, as will be appreciated the correlator 52 only receives one regenerated code word corresponding to first code word $X^{(1)}$ to form the similarity values for the set of n code words as illustrated in Figure 4.

As will be appreciated from the above explanation, if the code word contains N samples, then only N unique cyclic shifts are possible. Therefore, if the required population of code words is p , which is greater than N , then several base watermarks will be required. Each base watermark can be cyclically shifted to produce N unique code words.

If the watermarked image forms one of a plurality of images in, for example, a video sequence, then the same code word will be added to each of the images. As such, once the suspected code word has been identified using the Fourier transform correlator illustrated in Figure 6, then a subsequent correlation can be formed using the full correlation sum $sim(i)$ as explained above. However, because the suspected code

word has already been identified, then the correlation only needs to be performed once for the code word identified by the Fourier transform correlator shown in Figure 6.

As will be appreciated, instead of forming the conjugate of the Fourier transform of the regenerated first code word X^1 , the conjugate of the Fourier transform of the recovered code word could be formed. This is expressed by the second alternative of the Fourier transform correlator shown below:

$$F^{-1}[F(X)^* F(X^{(1)})]$$

Accordingly the conjugate of one of the Fourier transform of the recovered code word and the Fourier transform of the regenerated code word is formed by the Fourier transform processors 100, 102.

Secret Permutation of Code Words

One disadvantage of forming a code word from a cyclic shift of a first code word X^1 is that the security of the watermark may be compromised. This is because under a collusion attack two watermarked images are compared. If the same code word has been added to each image, with only a cyclic shift with respect to two versions of the same code word, an attacker may be more likely to identify the differences between the two marked material items and therefore identify the code word. With knowledge of the code word an attacker may either remove the watermark or alter the watermark to falsely implicate another.

In order to reduce the likelihood of a successful collusion attack, the order of each of the code word coefficients of each of the cyclically shifted code words is randomly permuted in accordance with a secret permutation code π . The permutation of the code word coefficients remains secret from the recipients of the marked images. Accordingly the likelihood of a successful collusion attack is reduced by an increase in the difficulty presented to a collusion attacker of identifying a correlation between two marked images.

At the detecting data processor the secret permutation code π will be known. In the detecting data processor, either the code word re-generator or the recovery processor 40 is operable to reverse the permutation π^{-1} of either the re-generated code word coefficients or the recovered code word coefficients in order to perform the correlation. The operation of the encoding data processor of Figure 1 and the detecting

data processor of Figure 2 is therefore as presented in a flow diagrams in Figures 7 and 8 respectively.

Watermark Code Word Generation

An improved implementation of watermark code word generation in accordance with an embodiment of the present invention will now be described with reference to Figures 9 and 10. As already explained, one of the advantages of generating code words by cyclically shifting a code word is that the Fourier transform correlator can be used to perform an efficient detector for the presence of a watermark code word in a marked material item.

As explained above, one disadvantage of generating code words from cyclically shifting a first code word X^1 is an increased vulnerability to collusion attack. As explained above, this vulnerability can be reduced by permuting the code word coefficients in accordance with a secret permutation code.

In order to reduce further the likelihood of a successful collusion attack, the code word generator performing part of the encoding image processor in preferred embodiments generates watermark code words having a plurality of differently generated parts. As will be explained, providing code words with a plurality of parts also provides a facility for generating a hierarchy of watermarks. As an illustration, a 20-bit code word is considered. The 20-bit code word provides over one million (1048576) possible data values.

In an illustrative embodiment the 20-bit code word is split into two 10-bit parts. This is shown in Figure 9. The first 10-bits are used to generate a first part of the watermark WM1. The second 10-bits are used to generate a second part of the watermark WM2. WM1 and WM2 are then embedded in the image to be watermarked as already explained.

In preferred embodiments WM1 may be formed by generating a single code word comprising first code word coefficients produced by the pseudo random number generator forming part of the code word generator 8. These numbers are generated from a base seed $SEED_{base}$ as illustrated in Figure 9. The base seed may be generated from samples of the source image.

For the first 10-bits of WM1 each of the 1024 possible data values are represented by 1024 possible shifts of the first part of the code word WM1 generated from the base seed. As illustrated in Figure 9 the shifts comprise 0 to 1023 possible values.

The second part of the watermark WM2 is generated in dependence upon the first part of the watermark WM1. The shift applied to WM1 is mapped onto one of 1024 possible supplementary seeds. Therefore the i -th shift of the code word $X^1 \rightarrow i = X_i^1$ identifies a unique supplementary seed (seed _{i}). From the supplementary seed a further code word is generated labelled in Figure 9 as X^2 . Thus there is a unique pre-determined relationship between the shift of the first code word X_i^1 forming WM1 and the seed used to form the second code word X_i^2 for WM2. However, in order to represent the further 1024 possible values, the second watermark WM2 is shifted in accordance with the 10-bit value for WM2. As shown in Figure 10, this provides a hierarchy of values. The first 1024 values provided by WM1 provides an indication of the code word forming WM2. The possible shifts of the code word formed from WM2 then provides a second set of 1024 values for a hierarchy of level two.

Embodiments of the present invention provide a facility for identifying watermarked images on the basis of plurality of hierarchies. For example, the WM1 can be used to identify the country, state or part of the state in which the images are distributed. The second level of the hierarchy can be used to identify a second part of the state, for example a town or cinema at which the watermarked images are reproduced. It will be appreciated that this can provide a facility for more quickly and more accurately identifying the location where the watermarked images were reproduced and from which offending copies were made.

A further advantage of generating code words having two parts WM1, WM2, is that the Fourier transform decoder shown in Figure 6 can be used to efficiently identify which of the 1024 values are present in each of the two hierarchical levels. In combination, since the second part of the watermark WM2 is formed from 1024 possible shifts of the second code word a further Fourier transform decoding can then be used to identify the possible shift of the second part of the code word WM2.

Forming the watermark code words having two related parts also provides an improvement in reducing the likelihood of a successful collusion attack. As explained above either or both code word parts may be permuted before being combined with the image.

Other Applications

In addition to the above-mentioned applications of the encoding data processing apparatus of the watermarking system to a cinema projector and to a web server, other applications are envisaged. For example, a receiver/decoder is envisaged in which received signals are watermarked by introducing code words upon receipt of the signals from a communicating device. For example, a set top box is typically arranged to receive television and video signals from a "head-end" broadcast or multi-cast device. As will be appreciated in this application, the encoding data processing apparatus forms part of the set top box and is arranged to introduce watermark code words into the video signals as the signals are received and decoded. In one example embodiment, the watermark code word is arranged to uniquely identify the set top box which receives and decodes the video signals.

In a further embodiment a digital cinema receiver is arranged to receive a digital cinema film via a satellite. The receiver is arranged to receive signals representing the digital cinema film and to decode the signals for reproduction. The receiver includes an encoding data processing apparatus, which introduces a watermark code word into the decoded film signals. The watermark code word is provided, for example, to uniquely identify the cinema receiving the film signals.

A further example embodiment may comprise a digital camera or camcorder or the like which includes a memory and a memory controller. An encoding data processing apparatus according to an embodiment of the present invention is arranged to introduce a watermark code word stored in the memory into video signals captured by the camera. According to this embodiment, the encoding data processing apparatus does not include a code word generator because the code word is pre-stored in the memory. Under the control of the memory controller the code word stored in the memory is embedded into the video signals, uniquely or quasi-uniquely identifying the video signals.

In a further embodiment, an encoding data processing apparatus according to an embodiment of the invention is operable encoded a sequence of watermark code words into different frames of digital images forming a continuous or moving picture. The code words may be related to one another and may be used to identify each of the images separately.

Various further aspects and features of the present invention are defined in the appended claims. Various modifications can be made to the embodiments herein before described without departing from the scope of the present invention.

4 Brief Description of Drawings

Figure 1 is a schematic block diagram of an encoding image processing apparatus;

Figure 2 is a schematic block diagram of a detecting image processing apparatus;

Figure 3A is a representation of an original image, Figure 3B is a representation of a marked image and Figure 3C is the marked image after registration;

Figure 4 is a graphical representation of an example correlation result for each of a set of code words N ;

Figure 5A is a graphical representation of samples of the original image I , Figure 5B is a graphical representation of samples of the watermarked image W' ; Figure 5C is a graphical representation of correlation results for the original image and the watermarked image with respect to discrete sample shifts;

Figure 6 is a schematic block diagram of a correlator forming part of the detecting data processing apparatus shown in Figure 2;

Figure 7 is a flow diagram of a process for forming watermarked images performed by the encoding image data processor;

Figure 8 is a flow diagram of a process for identifying a watermark from a received marked copy of the image performed by the detecting data processor of Figure 2;

Figure 9 is a schematic representation illustrating a process of forming code words having at least two parts; and

Figure 10 is a schematic representation illustrating the use of the code word with two parts formed in Figure 9 to provide a hierarchical information.

1 Abstract

A watermarking system comprises an encoding data processor operable to generate at least one marked version of an original item of material by introducing one of a predetermined set of code words into a copy of the original material item. The apparatus comprises a code word generator operable to provide the code word having a plurality of code word coefficients, and an encoding processor operable to combine the code word coefficients with the material. Each of the plurality of code words of the set is uniquely associated with a data word having first and second fields. Each of a set of values of the first field is represented as a first part of the code word having a first plurality of coefficients, and the second field is represented as a second part of the code word having a second plurality of coefficients.

The present invention provides a facility for generating watermark code words having a hierarchy of values. By providing watermark code words having first and second parts, a data word with first and second fields can be uniquely identified. The first and second fields can be assigned to different associated parameters such as for example address parameters. The first field could therefore identify the country of distribution of the material, whereas the second field could identify a particular distribution outlet within the country. A watermarking system can be formed, which finds particular application in identifying a point of distribution of pirate copies of video material generated by capturing the watermarked image, using, for example, a camcorder in a cinema.

2 Representative Drawing

[Fig 7]

【図1】

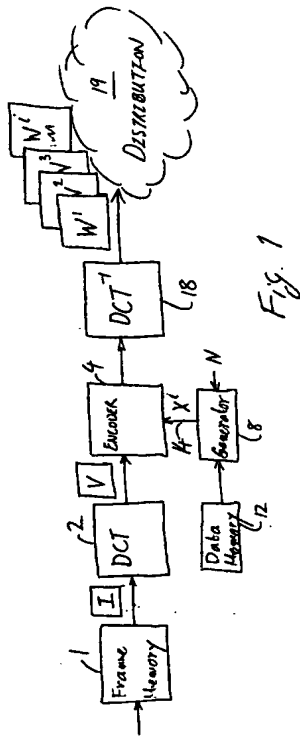


Fig. 1

【図2】

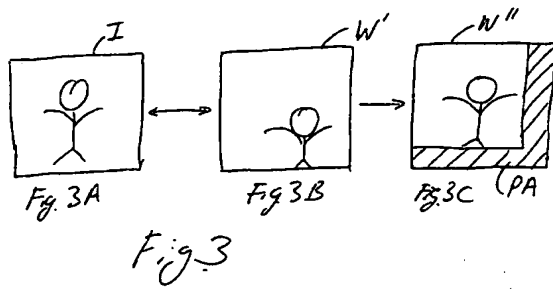


Fig. 3

【図4】

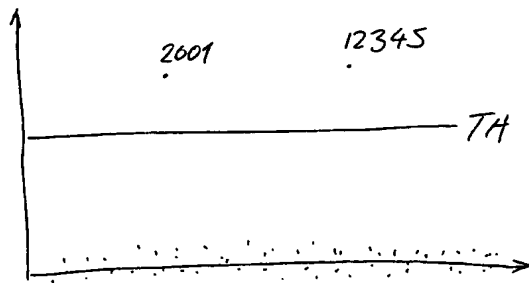


Fig. 4

【図5】

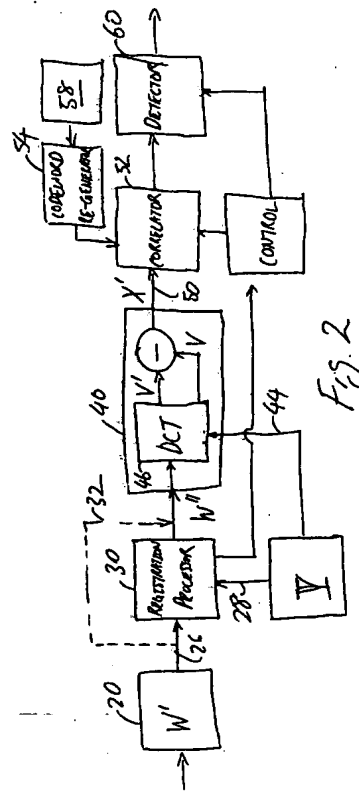


Fig. 2

【図3】

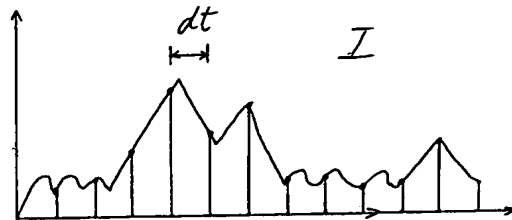


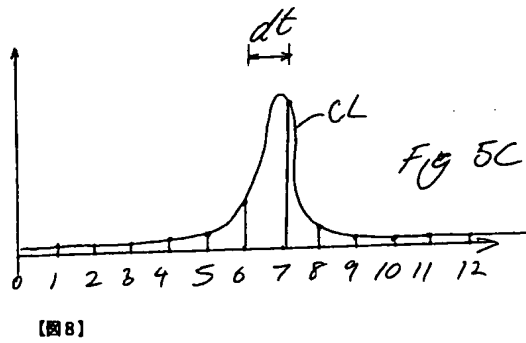
Fig. 5A

【図6】



Fig. 5B

【図7】



【図8】

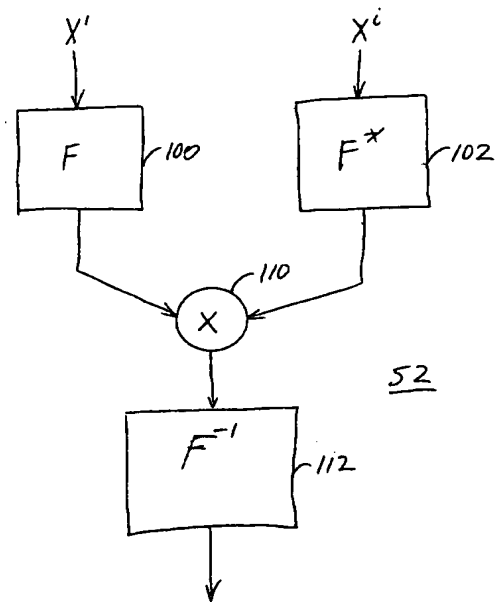


Fig. 6

【図9】

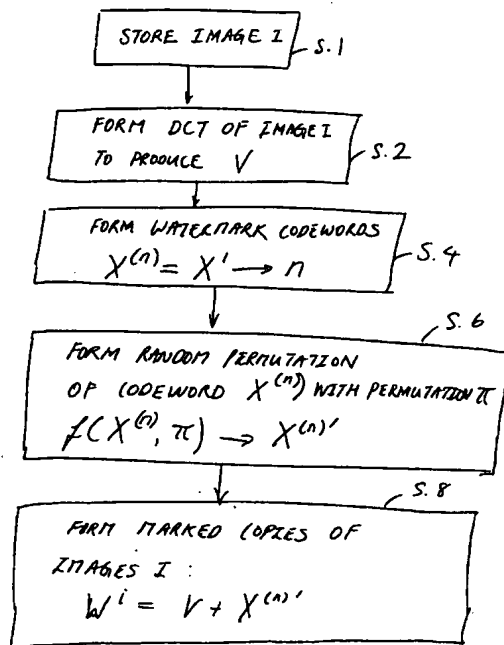


Fig. 7

【図10】

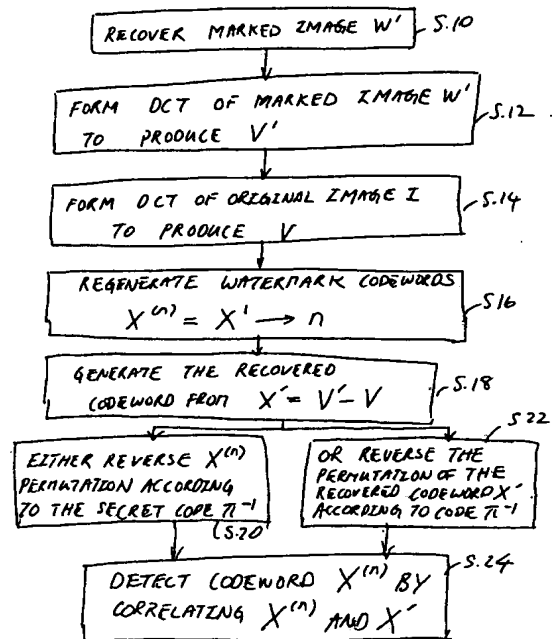


Fig. 8

【図11】

WATERMARK 1 (WM1)

10-BIT VALUE $\rightarrow 2^{10} = 1024$ VALUES

FORM $X' = \{x_0, x_1, x_2, x_3, \dots, x_n\}$ SEED_{base}

FORM $X'_i = X' \rightarrow i$

X'_0 0 SHIFT OF X'

X'_1 1 SHIFT OF X'

X'_2 2 SHIFT OF X'

X'_{1023} 1023 SHIFT OF X'

WATERMARK 2 (WM2)

10-bit $\rightarrow 2^{10} = 1024$ VALUES

SHIFT i OF $X' \rightarrow$ SEED_{shift} FOR WM2 $\rightarrow X^2$

$X^2 = \{x_0, x_1, x_2, x_3, \dots, x_n\}$ SEED_{supply}

SHIFT OF $X^2_i \rightarrow 1024$ POSSIBLE VALUES

Fig. 9

[012]

WM1 $\rightarrow \{0, 1, 2, 3, \dots, 1023\}$ LEVEL 1

E.G. LEVEL 1 \rightarrow COUNTRY OF DISTRIBUTION

WM2

WM2 $\rightarrow \{0, 1, 2, 3, \dots, 1023\}$ LEVEL 2

E.G. LEVEL 2 \rightarrow CINEMA WHERE FILM SHOWN

Fig. 10